The Army War College Review

Student Publications

UNITED STATES
ARMY WAR COLLEGE
PRESS

Carlisle Barracks, PA

STRENGTH *and* WISDOM

Selection Process

Research articles are selected from among award-winning student papers evaluated by the USAWC Distinguished Academic Chairs as outstanding exemplars of student writing or research at the professional graduate level. *Insight* articles are written primarily by AWC Fellows, studying off-site at prestigious institutions. The Student Awards Competition is open to all enrolled Resident Students, Distance Education Students, and AWC Fellows. Edited for economy, clarity, and impact.

USAWC Distinguished Academic Chairs

Cover

Flag flying over the Strength and Wisdom statue, a gift from the class of 2014, capturing the mission, spirit, and history of Carlisle Barracks (photo by Laura A. Wackwitz, Ph.D.).

Disclaimer

The United States Army War College
Student Publications

The Army War College Review

Volume 4 ▪ Numbers 1 & 2 ▪ 2018 Special Issue

Russian Exploitation of the Cyber Gap in International Law

Kenneth J. Biskner

The evolution of cyberspace into a domain of warfare has transformed the use of force by nation-states. Cyber-attacks can impose devastating consequences on an adversary without recourse to traditional kinetic violence. Recent history demonstrates that such attacks are no longer theoretical possibilities. Cyber-attacks against states have shut down power grids, disrupted financial markets, and even blockaded access to the Internet. The law of armed conflict, however, has not kept pace with this change in warfare, creating a gap in international law. The 2008 Russo-Georgian War exposes this gap and highlights the need for new international law to govern state sponsored cyber-attacks.

Keywords: *Cyber Warfare, Use of Force, Law of Armed Conflict, Georgia, Russia, Cyber-Blockade*

Russian foreign relations have assumed a disturbing dimension over the past decade, including coercive cyber-attacks by Russian proxies as a recurring tactic to further state interests. [1] Employment of the tactic typically begins with an unfavorable bilateral exchange between Russia and a neighboring state. When diplomacy fails to produce a favorable Russian outcome, the neighbor experiences intense Distributed Denial of Service (DDoS) and Denial of Service (DoS) cyber-attacks.[2] When confronted with evidence that the attacks are emanating from Russia, Russian officials

Kenneth J. Biskner (LL.M., U.S. Army Judge Advocate General School) is a Lieutenant Colonel in the United States Army. An earlier version of this article, written under the direction of Professor Douglas C. Lovelace, Jr., earned the prestigious **Army War College Foundation's Daniel M. Lewin Cyber** *-Terrorism Technology Writing Award for the USAWC class of 2017.*

[1] Robert Windrem, "Timeline: Ten Years of Russian Cyber Attacks on Other Nations," *NBC News Online* (December 18, 2016), http://www.nbcnews.com/news/us-news/timeline-ten-years-russian-cyber-attacks-other-nations-n697111; Harfn Steiner, *Coercive Instruments in the Digital Age: The Cases of Cyber-Attacks Against Estonia and Iran* (Stockholm, Sweden: Swedish National Defense University, Fall 2014), 44.

[2] A DoS cyber-attack uses one computer to attack a server with a flood of data packets. This overwhelms the server's capacity to respond, making it inaccessible to other users. A DDoS cyber-attack uses many hijacked computers (bots) networked together (botnet) and coordinated by a botmaster to attack a server. A botnet can have thousands of bots dispersed across the globe, making DDoS attacks more powerful than DoS attacks. Adrian Brindley, *Denial of Service Attacks and the Emergence of Intrusion Prevention Systems,* (Bethesda, MD: SANS Institute, November 1, 2002), 2, https://www.sans.org/reading-room/whitepapers/firewalls/denial-service-attacks-emergence-intrusion-prevention-systems-818.

attribute blame to spontaneous cyber-riots by patriotic Russians. Evidence from several such cyber-attacks, however, indicates the truth is far more complicated.

Patriotic Russians, although involved, are not the organizing force behind the cyber-attacks. The sophistication, coordination, and advanced preparation of these cyber-attacks far exceed what can be explained by spontaneous cyber-rioting. Far from impromptu, these attacks follow a pattern. First, highly sophisticated DDoS attacks are launched using botnets under the control of Russian organized cybercrime rings (cyber-mercenaries). Second, the cyber-mercenaries incite ordinary Russians to become cyber-rioters who engage in cyber-attacks against carefully selected targets. This crowdsourcing-style strategy leverages capabilities and helps establish state deniability. Once recruited, these cyber-rioters are armed with cyber-attack kits, provided target lists, and trained. They then engage in coordinated attacks. The cyber-rioters typically possess basic computer skills and have no experience hacking, but the process of weaponizing them is so simple that even a computer novice can begin launching DoS attacks in less than an hour.[3] Russian officials provide no assistance in halting these attacks or investigating them after the fact.[4] Based on this pattern, and other evidence, many experts agree that organized cybercrime rings are permitted to freely operate in Russia in exchange for state ordered cyber-attacks.[5]

Russia first employed this tactic against Estonia in 2007. Subsequent cyber-attacks following the pattern include: Lithuania 2008, Georgia 2008, Kyrgyzstan 2009, Kazakhstan 2009, and Ukraine in 2014.[6] Much has been written about the cyber-**attack on Estonia due to its novelty and Estonia's** membership in NATO. The Estonia case also raised many questions regarding the application of the law of armed conflict (LOAC) to cyber-attacks. A group of distinguished scholars was organized by NATO to study the problem and publish their findings. The result was the *Tallinn Manual*, which is considered the most authoritative pronouncement on the application of international law to cyberspace to date.[7] Unfortunately, the *Tallinn Manual* exposed a gap in international law that leaves all but the most severe state cyber-attacks virtually unregulated. Telecommunications technologies have far outpaced the evolution of the LOAC.[8] Attempts to apply existing law to cyber-attacks by analogy have proven inadequate because states are deeply divided on the meaning of essential terms. A common definition of what constitutes a use of force in cyberspace does not exist. Consequently, when states can engage in self-defense remains unclear. Similarly, states engaging in cyber operations do not know what conduct is prohibited by the United Nations Charter.

This essay places the problem in context by explicating and evaluating the LOAC using the Russo-Georgian War (the War) as a lens. The War highlights the failure of the LOAC to adequately regulate the vast majority of state-sponsored cyber-attacks. The LOAC should be updated with a cyber convention that closes this legal gap.

---

[3] Evgeny Morozov, "Army of Ones and Zeros: How I Became a Soldier in the Georgia-Russia Cyberwar," *Slate Online,* August 14, 2008, http://www.slate.com/articles/technology/technology/2008/08/an_army_of_ones_and_zeroes.html.

[4] Marching off to Cyberwar, *The Economist Online,* December 4, 2008, http://www.economist.com/node/12673385.

[5] Cory Bennett, "Kremlin's Ties to Cyber Gangs Sow US Concerns," *The Hill Online,* November 10, 2015, http://thehill.com/policy/cybersecurity/256573-kremlins-ties-russian-cyber-gangs-sow-us-concerns.

Andrew Foxall, "Putin's Cyberwar: Russia's Statecraft in the Fifth Domain," *Russian Studies Center at the Henry Jackson Society*, Policy paper No. 9 (May 2016): 11.

[6] Windrem, "Timeline."

[7] International Group of Experts, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (New York: Cambridge University Press, 2017).

[8] Michael N. Schmitt and Liis Vihul, "Tallinn Paper No. 5: The Nature of International Law Cyber Norms," *NATO Cooperative Cyber Defense Center of Excellence*, (2014): 31

Law of Armed Conflict

The LOAC has evolved into two distinct bodies of law—*jus ad bellum* and *jus in bello*—that reflect the moral aspects of war. *Jus ad bellum* governs the just basis for states to resort to the use of armed force.[9] *Jus in bello* regulates the means and methods states may lawfully employ in the use of armed force.[10] This paper is limited to discussion of the first, *jus ad bellum*, because it sets the threshold determination for the application of the LOAC to any conflict (i.e., the existence of an armed conflict). *Jus ad bellum* analysis is especially challenging in the case of cyber-attacks because (a) they are difficult to define, and (b) only a very small category of cyber-attacks is considered a use of armed force governed by international law.

Jus ad bellum is comprised of two essential elements: necessity and proportionality.[11] Necessity requires states to resort to the use of armed force only as a last resort to prevent an imminent attack or stop one in progress.[12] Proportionality requires states to limit the use of armed force to the amount required to prevent an imminent attack or stop one in progress.[13] Both principles have been incorporated into two articles of the UN Charter which provides the modern framework for the lawful use of armed force between states.[14]

The Use of Force

The United Nations was established in 1945 to preserve international peace and suppress aggression.[15] The UN Charter achieves this with the following provisions:

- Article 2(4): All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state.
- Article 51: Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations.[16]

In short, Article 2(4) outlaws aggressive war and Article 51 provides an exception to the rule for self-defense. **Unfortunately, the UN Charter does not define the terms "use of force" or "armed attack."** Although some meaning can be derived from other sources of international law, both terms are inherently ambiguous.

Article 2(4) outlaws a broad spectrum of coercive conduct between states, with high-intensity armed conflicts constituting a clear use of force. In contrast, the low end of the spectrum is relatively unknown. The UN Charter was not designed with low-intensity or unconventional conflicts (e.g., cyber warfare) in mind, so state conduct that does not resemble classic military violence is particularly difficult to characterize.

Article 51 authorizes the use of force in response to armed attacks. Accordingly, an armed attack is a condition precedent to the lawful use of force in the absence of UN Security Council

---

[9] Stephen W. Preston, *Law of War Manual* (Washington, DC: U.S. Department of Defense, May 2016), 39.

[10] Ibid., 39.

[11] Ibid.

[12] Michael N. Schmitt, Cyber Operations and the Jus Ad Bellum Revisited, *Villanova Law Review* 56, no. 3 (2011): 593.

[13] Ibid., 593.

[14] Preston, *LOW Manual*, 42.

[15] U.N. Charter, Article I.

[16] U.N. Charter, Articles 2(4) and 51.

authorization.[17] The term armed in this context is commonly understood to mean the employment of military weapons.[18] **International law defines an attack as an "[act] of violence against an adversary."**[19] The precise meaning of the two terms together is a matter of debate; however, violence resulting in injury/death or damage/destruction of tangible objects may suffice.[20] An armed attack is a higher threshold than a use of force under Article 2(4), with the distinguishing factor being the intensity of the violence.[21] Unfortunately, the degree of intensity necessary to constitute an armed attack is unclear.

A use of force that falls below the threshold of an armed attack represents an undefined gray area.[22] Examples of state conduct that lie along the spectrum of coercive state acts add some clarity. For example, economic and political coercion and countermeasures[23] fall below the threshold of a use of force.[24] Other forms of state conduct, while being illegal under domestic or international law, are also recognized as not constituting a use of force (e.g., espionage, subversion, unarmed intervention).[25] In *Nicaragua v. United States,* the International Court of Justice (ICJ) opined that funding insurgents was not a use of force.[26] Training and equipping insurgents and border skirmishes, however, are uses of force that lack the intensity of an armed attack.[27] At the right end of the spectrum detailed in Figure 1, the use of airplanes as weapons on September 11, 2001, was declared an armed attack.[28]

FIGURE 1: UN Charter Spectrum of Coercion

---
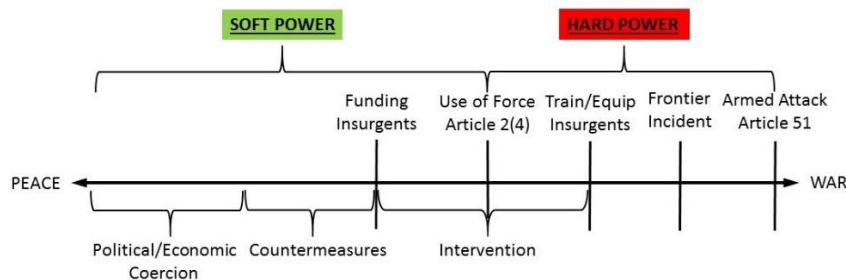
[17] Michael N. Schmitt, "Attack as a Term of Art in International Law: The Cyber Operations Context," *4th International Conference on Cyber Conflict* (Tallinn, Estonia: NATO CCD COE Publications, 2012), 285.

[18] Ibid., 283.

[19] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of the Victims of International Armed Conflicts, Article 49(1) (June 8, 1977).

[20] Michael N. Schmitt, "The Use of Force in Cyberspace: A Reply to Dr. Ziolkowski," *4th International Conference on Cyber Conflict* (Tallinn, Estonia: NATO CCD COE Publications, 2012), 314.

[21] *Military and Paramilitary Activities in and Against Nicaragua* (Nicaragua v. U.S.), 1986 I.C.J. 14 (June 27), para. 195.

[22] Ashley Deeks, "Multi-Part Tests in the Jus Ad Bellum," *Houston Law Review* 53, no. 4 (2016): 1053.

[23] Countermeasures are non-forceful acts (normally prohibited by international law) by a state to cause another state to cease internationally wrongful acts. The classic example in response to cyber-attacks is hacking back. International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts,* U.D. Document A/56/10 (2001) http://www.refworld.org/docid/3ddb8f804.html.

[24] Daniel B. Silver, "Computer Network Attack as a Use of Force Under Article 2(4) of the United Nations Charter," *International Law Studies* 76, (2002): 80.

[25] Priyanka R. Dev, "Use of Force" and "Armed Attack" Thresholds in Cyber Conflict: The Looming Definitional Gaps and the Growing Need for Formal U.N. Response," *Texas International Law Journal* 50, no. 2 (2015): 393.

[26] *Nicaragua*, para 195.

[27] Ibid.

[28] United Nations Security Council Resolution 1368: 4370th Meeting, UN Doc. S/RES/1368 (September 12, 2001).

Applying the LOAC to Cyber-Attacks

Because the UN Charter's framework for regulating armed conflict is frozen in World War II notions of force, it does not account for new technologies that exert little to no force in the historic sense.[29] In the physical domains, for example, a use of force is a violent act that produces a kinetic effect that is easily recognizable. Cyber-attacks, in contrast, are non-violent and any kinetic effect is indirect, making detection difficult. As a result, no common definition for the use of force via cyberspace exists.[30] Since the LOAC only applies to armed conflicts, it does not address the vast majority of state cyber-attacks where violent effects are unclear if not lacking altogether. Despite this, the LOAC has not been updated to account for the evolution of cyberspace into a domain of warfare.[31]

To address the problem, the UN organized a group of governmental experts (GGE) in 2004 to build consensus for international cybersecurity norms. In 2013, the GGE reached consensus on the application of the international law to state conduct in cyberspace. This appears to have resolved the question of whether *jus ad bellum* applies to cyber-attacks.[32] The GGE, however, has not clarified how international law applies to cyberspace nor defined essential terminology. The unique characteristics of cyberspace complicate *jus ad bellum* determinations and currently no agreement exists regarding what constitutes a "cyber-attack,"[33] leaving the application of already ambiguous legal concepts to cyberspace a matter of ongoing debate.[34]

Cyberspace: The U.S. Department of Defense (the DoD) designated cyberspace a new domain of warfare in 2010,[35] but a clear understanding of what it is remains elusive. The scope and artificial nature of the cyberspace makes it difficult to define by analogy to other domains.[36] This uniqueness affects the application of the LOAC in a material manner. First, situational awareness is the lowest of all domains. Defenders have difficulty knowing when an attack has occurred and what the motive of the attacker was.[37] A network intrusion, for example, may remain undetected for a long period of time and it may be unclear whether the purpose of the intrusion was cybercrime, espionage, or war. Next, actors can easily conceal their identities through technical means.[38] Articles 2(4) and 51 generally only apply to attacks by states, so the difficulty of attributing a cyber-attack to its source is a major challenge.

Cyber Attack: The term cyber-attack is loosely used to describe a spectrum of unlawful conduct in cyberspace that ranges from ordinary crime committed by individuals to armed attacks perpetrated by states.[39] The result is confusing rhetoric that dangerously conflates all malicious cyber conduct with a state of war.[40] In order to separate conduct prohibited by the UN Charter from other types of cyber-attacks, it is necessary to distinguish the motives and types of actors. Cyber-attacks

---

[29] Reese Nguyen, "Navigating Jus Ad Bellum in the Age of Cyber Warfare," *California Law Review* 101, no. 2 (August 3, 2013):1118.

[30] Schmitt, "Attack as a Term of Art," 290.

[31] Preston, *LOW Manual*, 985.

[32] "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security:" 68th Session, UN Doc. A/68/98, (June 24, 2013): 8.

[33] Mehdi Kadivar, "Cyber-Attack Attributes," *Technology Innovation Management Review*, (November 2014): 23.

[34] Schmitt, "Cyber Operations," 569; James E. McGhee, "Cyber Redux: The Schmitt Analysis, Tallinn Manual and US Cyber Policy," *Journal of Law and Cyber Warfare* 2, no. 1 (2013): 64.

[35] Robert M. Gates, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2010): 37.

[36] Welton Chang and Sarah Granger, "Warfare in the Cyber Domain," *Air and Space Power Journal*, September 2012, 1.

[37] Jeffrey L. Caton, *Information Operations Primer* (Carlisle Barracks, PA: US Army War College: 2011), 19.

[38] Ibid., 19.

[39] Oona A. Hathaway, Rebecca Crootof, et al., "The Law of Cyber Attack," *California Law Review*, (2012): 823.

[40] Laurie R. Blank, "Cyberwar Versus Cyber Attack: The Role of Rhetoric in the Application of Law to Activities in Cyberspace," *in Cyberwar: Law and Ethics for Virtual Conflicts*, ed. Jens Ohlin, Claire Finkelstein and Kevin Govern (Oxford: Oxford University Press, 2015), 97.

can be segregated into five overlapping groups: cybercrime, cyber-terror/insurgency, cyber-attacks, cyber use of force, and cyber armed attacks.

FIGURE 2: Cyber-Attack Relationships
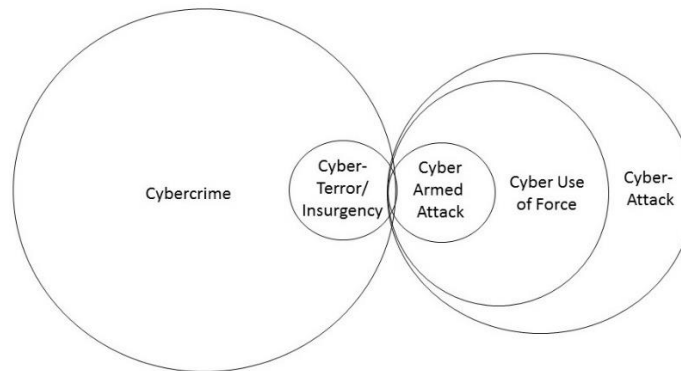
Cybercrime Sphere

Attacks in the cybercrime sphere are perpetrated by non-state actors, are largely governed by domestic law, and do not constitute Article 51 armed attacks. Accordingly, this conduct falls outside **the UN Charter's framework.**

Cybercrime is a violation of domestic criminal law carried out for enrichment or other personal motives via computer code that affects the normal function of an electronic device or its data.[41] This conduct is harmful to individuals or organizations and includes acts like fraud, theft, and hacking.[42] Cybercrime represents the majority of unlawful conduct on the internet and was estimated to cost the global economy $3 Trillion in 2015.[43] This cost is projected to double by 2021 as the Internet of Things expands and cybercrime evolves.[44]

Cyber-terror and cyber-insurgency are a subset of cybercrime defined as the violation of **domestic criminal law carried out "with the intention to cause harm or further social, ideological,** religious, political or similar objectives, or to intimidate any person in furtherance of such objectives" via computer code that affects the normal function of an electronic device or its data .[45] No significant acts of cyber-terrorism or cyber-insurgency against critical infrastructure are publicly known to have occurred.[46] The threat of such attacks, however, is an increasingly high national security concern as actors gain sophistication.[47]

---

[41] Cameron S.D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice," *International Journal of Cyber Criminology* 9, no. 1 (January – June 2015): 57.

[42] James McGhee, "Hack, Attack or Whack; The Politics of Imprecision in Cyber Law," *Journal of Law and Cyber Warfare* 4, no.1 (Spring 2014): 20.

[43] Steve Morgan, "Cybercrime Damages Expected to Cost the World $6 Trillion by 2021: Massive Expansion of the Global Cyber Attack Surface Will Fuel the Cybercrime Epidemic," *CSO Online* (August 22, 2016), http://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html.

[44] Ibid.

[45] Catherine A. Theohary and John W. Rollins, *Cyberwarfare and Cyberterror: In Brief* (Washington, DC: U.S. Library of Congress, Congressional Research Service, March 27, 2015), ii.

[46] Thomas M. Chen, *Cyberterrorism After STUXNET* (Carlisle Barracks, PA: Strategic Studies Institute, June 2014), 20.

[47] Abdulrahman Alqahtani, "Awareness of the Potential Threat of Cyberterrorism to the National Security," *Journal of Information Security*, (October 2014): 145.

Cyber-Attack Sphere

Various activities in the cyber-attack sphere that are perpetrated by state actors and may be governed by international law. Such activity is coercive state conduct that affects the sovereignty or national interests of the victim state. Accordingly, these attacks provide a basis for *jus ad bellum* analysis.

Cyber-attacks are a broad category of state conduct executed via computer code to affect an electronic device or its data for political or national security purposes.[48] Conduct in this category may or may not undermine the normal function of the electronic device. The members of the Shanghai Cooperation Organization, for example, define cyber-attacks broadly to include conduct that western states would consider essentially free speech.[49] The principle of non-intervention in the UN Charter, however, generally prohibits such conduct if it has a coercive effect.[50]

Cyber use of force is an attack by a state actor via computer code that negatively affects the normal function of an electronic device or its data for political or national security purposes and produces kinetic effects that result in injury/death or damage/destruction of tangible property.[51] Such attacks constitute a use of force under Article 2(4) of the UN Charter, but because the exact nature of this conduct is unknown, many states like Russia exploit this gap in international law.

Cyber armed attack is an attack by a state actor via computer code that negatively affects the normal function of an electronic device or its data for political or national security purposes and produces kinetic effects that result in injury/death or damage/destruction of tangible property with scale and effects similar to classical forms of warfare. This very small subset of cyber-attacks is not yet publicly known to have occurred. However, the consensus among the International Group of Experts (IGE) who participated in the drafting of the *Tallinn Manual* is that such attacks do trigger the inherent right to self-defense under Article 51.[52]

Framework for Analysis

Scholars have proposed several frameworks to determine whether a use of force has occurred, with a consensus around a model known as the effects-based approach. This model is superior because it strikes a balance between the alternative approaches which are either too restrictive or too inclusive.[53] The effects-based framework focuses on the consequences of cyber-attacks, enabling states to evaluate the degree to which vital interests have been impacted.[54] This is consistent with DoD policy which provides that **states must evaluate "t**he effect and purpose**" of cyber**-attacks.[55] Despite its many strengths, however, the effects-based framework suffers from the subjective nature

---

[48] Hathaway, "The Law of Cyber Attack," 826.

[49] Shanghai Cooperation Organization, "Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security," 61st Plenary Meeting, (December 2, 2008): 203.

[50] Ido Kilovaty, "Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare," *National Security Law Brief* 5, no. 1 (2014): 107.

[51] Hathaway, "The Law of Cyber Attack," 826.

[52] IGE, *Tallinn Manual*, 339.

[53] Noah Simmons, "A Brave New World: Applying the International Law of War to Cyber-Attacks, *Journal of Law and Cyber Warfare* 4, no.1 (Winter 2014): 60.

[54] Andrew C. Foltz, "Stuxnet, Schmitt Analysis, and the Cyber "Use-of-force" Debate," *Joint Force Quarterly,* no. 67 (4th Quarter 2012): 41.

[55] Leon Panetta, *Cyberspace Policy Report: A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934* (Washington, DC: Department of Defense, November 2011), 9.

of the criteria used to evaluate an attack's "scale and effects."[56] Reasonable observers can reach wildly different conclusions on the same set of facts, calling into question the model's reliability.[57] Despite this weakness, the effects-based framework is the most thorough and effective tool currently available for the analysis of cyber-attacks.

Under the Schmitt model—the most widely accepted version of the effects-based framework—seven criteria are analyzed to determine whether a cyber-attack constitutes a use of force under Article 2(4): severity, immediacy, directness, invasiveness, measurability, legitimacy, and responsibility.[58] The IGE adopted this approach in their commentary for Rule 69, while adding the additional criteria of military character.[59] It should be noted, however, that these criteria do not constitute a legal test; rather, they are factors states consider in making *jus ad bellum* determinations.[60]

- Severity: The degree of **harm caused in light of an attack's scale, scope, intensity, duration,** and effects. Cyber-attacks that result in effects similar to those associated with conventional uses of armed force (property damage, personal injury, death, or destruction) are more likely to constitute a use of force. Severity is weighted the most heavily of all the criteria.[61]
- Immediacy: Cyber-attacks that produce effects quickly, leaving victim states little time to react, are more likely to be a use of force.
- Directness: The more proximate the effects of a cyber-attack are to consequences, the more likely it is a use of force.
- Invasiveness: The more a cyber-attack violates the sovereignty of the victim state, the more likely it is a use of force.
- Measurability: The more clearly the effects of a cyber-attack manifest in objective metrics, the more likely it is a use of force.
- Legitimacy: State conduct in cyberspace that does not represent a use of force (espionage, propaganda, economic/political coercion) is presumed legitimate.
- Responsibility: The more a state is involved in cyber-attack, the more likely it is a use of force.[62]
- Military Character: The more proximately a cyber-attack is linked to military operations, the more likely the attack is a use of force.[63]

The Russo-Georgian War: A Case Study

Georgia is located in the South Caucasus region and covers an area approximately the size of Virginia. **Geopolitically, it serves as a buffer zone between Russia's southern border and Turkey (a** NATO member). Georgia also controls strategic transit routes through the Caucasus Mountains and

---

[56] James E. McGhee, "Cyber Redux: The Schmitt Analysis, Tallinn manual and US Cyber Policy," *Journal of Law and Cyber Warfare* 2, no. 1 (2013): 64.

[57] Silver, "Computer Network Attack," 89.

[58] Michael N. Schmitt, "Cyber Operations and the Jus Ad Bellum Revisited," *Villanova Law Review* 56, no. 3 (2011): 569. Professor Michael N. Schmitt, LLM, JD, Chairman, International Law Department, U.S. Naval War College. Professor Schmitt is perhaps the foremost scholar on the application of the LOAC to cyber-warfare and is the editor of the Tallinn Manual.

[59] IGE, *Tallinn Manual*, 334-336.

[60] Ibid, 333.

[61] Schmitt, "Cyber Operations," 576.

[62] Ibid., 576-577.

[63] IGE, *Tallinn Manual*, 50.

pipelines that carry oil and gas from the Caspian Sea to the Black Sea. These factors accord Russia vital national security and economic interests in the region.[64]

Georgia also has a long history with Russia as a Soviet Republic and client state within the Russian Empire. **Georgia's 1991 transition to independence was complicated by claims of autonomy** by its Abkhazia and South Ossetia regions (the Regions), a status the Regions enjoyed under Soviet rule. Georgia attempted to reassert its sovereignty with occupying forces, but the policy escalated long-simmering tensions into open rebellion.[65] In 1992, Russia and Georgia established a joint peacekeeping force to restore order. **The Russian "peacekeepers," however, were** essentially an occupying force to secure Russian strategic interests.[66]

The 2003 Rose Revolution radically changed the Georgian government, shifting the country out of the Russian sphere of influence and aligning it with the West. In response, Russia established a de facto annexation of the Regions by extending Russian citizenship to the Separatists.[67] In response, Georgia attempted unsuccessfully to reintegrate the Regions with guarantees of autonomy.[68] The impasse prompted Georgia to initiate international talks for the replacement of Russian peacekeepers with a multi-national force.[69] Unfortunately, the international community offered little **assistance and the effort deteriorated Georgia's already poor relations with Russia.**

Tensions remained high but manag**eable until Kosovo's declaration of independence on February** 17, 2008. **International recognition of Kosovo's independence provided Russia the pretext it needed** to recognize the independence of the Regions and thereby cement Russian control.[70] Russia began preparing for armed conflict with Georgia about this time by moving thousands of troops into the Regions, prepositioning war material, and improving transportation infrastructure essential to rapidly moving troops.[71] From July 5 to August 2, Russia also conducted a large scale military exercise in the area with 8,000 troops. One exercise scenario was a Russian counter-attack into the Regions to repel Georgian forces.[72] When the exercise ended, Russian forces remained in place and on alert.[73] In hindsight, the Russians used the exercise as an elaborate rehearsal for the invasion of Georgia.[74] Taken together, these actions suggest that Russia expected its peacekeeping role to transform into an armed conflict—the only thing missing, however, was a justification for the use of armed force.

Georgia successfully defused provocations by Abkhaz Separatists in the first half of 2008. By midyear, however, a series of incidents with South Ossetian Separatists had escalated. The

---

[64] Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgian War: Lessons and Implications* (Carlisle Barracks, PA: Strategic Studies Institute, June 2011), 1-3.

[65] Human Rights Watch, "Georgia/Abkhazia: Violations of the Laws of War and Russia's Role in the Conflict," *Human Rights Watch Arms Project* 7, no. 7 (March 1995): 17.

[66] Svante E. Cornell and S. Frederick Starr, *The Guns of August 2008: Russia's War with Georgia* (New York: Routledge, 2009), 131.

[67] Kristopher Natoli, "Weaponizing Nationality: An Analysis of Russia's Passport Policy in Georgia," *Boston University International Law Journal* 28, no. 2 (Summer 2010): 389.

[68] Cohen, *"The Russian Military,"* 5.

[69] Svante E. Cornell, Johanna Popjanevski and Niklass Nilsson, "Russia's War in Georgia: Causes and Implications for Georgia and the World," *Central Asia-Caucasus Institute* (August 2008): 9.

[70] Gregory Hafkin, "The Russo-Georgian War of 2008: Developing the Law of Unauthorized Humanitarian Intervention after Kosovo," *Boston University International Law Journal* 28, no.1 (Spring 2010): 221.

[71] Cornell, *The Guns of August*, 154.

[72] Ria Novosti, "Georgia Protests Russian Military Drills in North Caucasus," *Asia-Plus Online,* July 17, 2008, http://news.tj/en/news/georgia-protests-russian-military-drills-north-caucasus.

[73] Ronald D. Asmus, A Little War that Shook the World: Georgia, Russia, and the Future of the West (New York: St. Martin's Press, 2010), 165.

[74] Jim Nichol, *Russia-Georgia Conflict in August 2008: Context and Implications for U.S. Interests* (Washington DC: U.S. Library of Congress, Congressional Research Service, March 3, 2009), 4.

Separatists shelled Georgian villages on August 1st, continuing the attacks intermittently for seven days without interference from Russian peacekeepers. A peace conference was arranged for August 7th, but the South Ossetian and Russian delegations did not appear. Georgia immediately announced a unilateral ceasefire to defuse the situation, but the Separatist attacks continued and thousands of regular Russian troops traversed the mountains into South Ossetia in preparation for an invasion.

On August 8th, Georgia sent troops into South Ossetia to stop the shelling and block the Russian invasion.[75] Georgian forces, outgunned and outnumbered by the Russians, were in full retreat the next day. On August 10th, Georgian forces had withdrawn from South Ossetia and the Georgian government announced another unilateral ceasefire. Despite this, Russian forces continued advancing to the central Georgian town of Gori, seizing control of the east-west transportation network, ejecting Georgian peacekeepers from Abkhazia, and seizing key territory in western Georgia. Combined with occupation of Gori, the western half of the country was firmly under Russian control. Russian forces destroyed targets in Western Georgia until they began withdrawing back into the Regions on August 22nd. Four days later, in what would become the defining moment in the conflict, Russian recognized Abkhaz and South Ossetian independence.

Ultimately, the War achieved several Russian strategic goals: (1) thousands of regular Russian troops were permanently based in the Regions to secure Russian interests; (2) the conflict undermined confidence in Georgian oil and gas pipelines, causing a shift in the transport of Caspian Sea petroleum products to Russian pipelines; and (3) Russia sent a clear warning to NATO and neighboring states that further NATO expansion along its borders was a red line.

Analysis: The Georgia Attacks

While tensions between Georgia and the Separatists were escalating on the ground in July and August of 2008, events were also unfolding in cyberspace. An integrated cyber campaign, that followed the Russian pattern of physical conflict during the war, accompanied operations in the physical domain. On July 19th, a relatively new server (located in the U.S.) was used to coordinate a DDoS attack on **the Georgian President's website.**[76] The server had a Russian registration and the botnet involved had not previously been employed.[77] Cybersecurity experts determined that software involved in the attack was characteristic of Russian hackers.[78] Like the counterpart Russian military exercise in July, the timing and nature of the attack indicate it was also a rehearsal for later operations.[79]

Investigations of the Georgia Attacks revealed a level of detail and preparation that far exceeded what can be explained by a spontaneous cyber-riot. Cyber reconnaissance started several weeks in advance of kinetic operations.[80] This work prepared the cyber battlespace by mapping Georgian networks, identifying weaknesses, and developing target lists.[81] One analyst noted that **"[t]he level of** advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the

---

[75] Cornell, *The Guns of August*, 170.

[76] Steven Adair, "The Website for the President of Georgia Under Attack - Politically Motivated?" *Shadowserver Foundation Online,* July 20, 2008, https://www.shadowserver.org/wiki/pmwiki.php/Calendar/20080720.

[77] Ibid.

[78] Ibid.

[79] Andreas Hagan, "The Rᴜssᴏ-Georgian War 2008: The Role of the Cyber Attacks in the Conflict," *Armed Forces Communications and Electronics Association,* May 24, 2012, 4.

[80] Hollis, "Cyberwar Case Study: Georgia 2008," 4.

[81] Brian Krebs, "Russian Hacker Forums Fueled Georgia Cyber Attacks," *The Washington Post Online,* October 16, 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.

assault by officials within the Russian government and or military."[82] Whatever the identity of the hackers, the level of preparation for the Georgia Attacks demonstrates that they were anything but spontaneous and disorganized. Further, the preparation reveals advanced knowledge of the coming Russian kinetic operations—knowledge they could only get from Russian officials.

Many cyber experts also conclude that the Russian Business Network (RBN) (a notorious Russian cybercrime organization) served as the cyber-mercenaries in this case. The RBN is known to contract for cybercrime services (including DDoS attacks) with third parties.[83] Analysis of the Georgia Attacks revealed that on August 7th, the RBN rerouted Georgian web traffic through Russian and Turkish servers under its control.[84] Later analysis determined that the malware used in the Georgia Attacks was found on these RBN controlled servers.[85] The RBN is a prime example of a known cybercrime organization permitted to operate by the Russian government and substantial evidence points to the RBN as the organizing force behind the Georgia Attacks.

When kinetic operations began on August 8th, widespread cyber-attacks were affecting targets across Georgia.[86] The Georgia Attacks followed the established Russian pattern.[87] First, the RBN directed DDoS attacks against Georgian targets (media outlets, government websites, and communications networks) in support of kinetic operations. Russian servers coordinated the attacks by RBN controlled botnets.[88] Next, the RBN incited ordinary Russians on social media sites.[89] These cyber-rioters were organized and directed by the RBN via two Russian hacker websites (xaker.ru and stopgeorgia.ru).[90] The RBN trained and armed the cyber-rioters with malware customized in advance for Georgian targets.[91] Malware similar to the attack kits was known to have been used by the RBN in the past.[92] Georgian cyber-defenses were quickly overwhelmed and by August 10th, virtually all government websites were offline.[93] The cyber-blackout lasted for a total of twenty days.

Severity: Evaluating the severity of the Georgia Attacks is complicated by the fact that DDoS and DoS attacks cause no physical damage to targeted systems. Access to blocked websites can be restored relatively quickly once such cyber-attacks end. This would appear to forestall states from engaging in self-defense no matter how severe the effects of DDoS and DoS attacks. The disruption of communications and economic activity dependent on the internet did impose costs on Georgia, however. The analogous case in international law is the blockade. Blockades exert no kinetic force, but nonetheless, constitute a use of force.[94]

---

[82] Ibid.

[83] Hagan, "The Russo-Georgian War," 16.

[84] Jart Armin, "RBN – Georgia Cyber Warfare," blog entry posted August 16, 2008, http://rbnexploit.blogspot.com/2008/08/rbn-georgia-cyberwarfare-2-sat-16-00.html.

[85] Hagan, "The Russo-Georgian War," 16.

[86] Stephen W. Korns and Joshua E. Katsenberg, "Georgia's Cyber Left Hook," *Parameters,* 38, no. 4 (Winter 2008-09): 60.

[87] Andrzej Kozlowski, "Comparative Analysis of Cyber Attacks on Estonia, Georgia and Kyrgyzstan," *European Scientific Journal* 3, (February 2014): 240; William C. Ashmore, *Impact of Alleged Russian Cyber Attacks,* (Fort Leavenworth, KS: School of Advanced Military Studies, May 21, 2009), 13.

[88] John Bumgarner and Scott Borg, *Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008* (U.S. Cyber Consequences Unit, August 2009), 3.

[89] Ibid., 3.

[90] Jart Armin, "RBN – Russian Cyber War on Georgia: Report," blog entry posted August 10, 2008, http://rbnexploit.blogspot.com/2008/10/rbn-russian-cyberwar-on-georgia.html.

[91] Bumgarner, *Overview by the US-CCU,* 3; Kozlowski, "Comparative Analysis," 240.

[92] Hagan, "The Russo-Georgian War," 16.

[93] Korns, "Georgia's Cyber," 60.

[94] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force," *Journal of National Security Law and Policy Online* 4, no. 63 (August 13, 2010): 72, http://jnslp.com/2010/08/13/offensive-cyber-operations-and-the-use-of-force/;

Blockades that may foreseeably result in a 3-5% loss of Gross Domestic Product have been recognized as armed attacks.[95] A cyber-blockade of sufficient severity may similarly invoke a state's right to self-defense,[96] but, determining the value of lost economic opportunities in such a case is extremely difficult.[97] Thirty-five percent of Georgian networks were offline during the 20 day cyber-blockade and another 60% were unstable.[98] Most notably, all electronic banking transactions were suspended for 10 days.[99] Approximately 24% of Georgians had internet access in 2008, so the Georgia Attacks unquestionably had some negative impact on economic activity.[100] Studies have demonstrated a direct correlation between GDP and internet penetration.[101] Further, the World Bank statistics reveal a rapid decline in Georgian GDP growth from 12.3% in 2007, to 2.3% in 2008, and a historic low of -3.8% in 2009.[102] Much of this economic decline can be attributed directly to the War. Unfortunately, no data is available to indicate what the actual cost may have been, or what part of the loss can be reasonably ascribed to the cyber-blockade.

Immediacy: The Georgia Attacks were immediate and afforded Georgia no time to prepare. Georgian cyber actions were reactionary and focused largely on reestablishing communications.

Directness: The Georgia Attacks directly impacted the economy by denying people access to financial services and interfering with commerce. Economic impact also included the effects of lost opportunities rippled outward causing additional economic losses.

Invasiveness: The Georgia Attacks were highly invasive, targeting government and financial sector networks. The effects on these systems were more than a mere inconvenience; the Georgia Attacks interfered with economic activity and the government's ability to communicate with the people during a national crisis.

Measurability: Measurability of the Georgia Attacks is low because of the subjective nature of valuing lost economic opportunities. Further, separating the economic impacts of the Georgia Attacks from those caused by kinetic operations may not be possible.

Legitimacy: The Georgia Attacks were not legitimate. Unauthorized blockades are illegal acts of aggression.[103] A majority of the IGE agrees that the law of blockades applies to cyber-blockades.[104]

Responsibility: While experts agree that no direct evidence linking the Russian government and the Georgia Attacks,[105] enough circumstantial evidence exists to make such a conclusion more likely than not.

Jason Barkham, "Information Warfare and International Law on the Use of Force," *New York University Journal of International Law and Policy* 57 (2001): 91.

[95] Sheng Li, "When does Internet Denial Trigger the Right of Armed Self-Defense?" 38 *Yale Journal of International of International Law* 38, (2013): 199.

[96] Ibid., 191.

[97] Alison L. Russell, *Cyber Blockades* (Washington, DC: Georgetown University Press, 2014), 108.

[98] Russell, *Cyber Blockades*, 104.

[99] Eneken Tikk, Kadri Kaska, and Liis Vihul*, International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2010), 78.

[100] International Telecommunications Union, Estimated Internet Users per 100 Inhabitants, https://www.itu.int/ITU-D/ict/statistics/material/excel/EstimatedInternetUsers00-09.xls.

[101] Shahram Amiri and Brian Reif, "Internet Penetration and its Correlation to Gross Domestic Product: An Analysis of the Nordic Countries," *International Journal of Business, Humanities and Technology* 3, no. 2 (February 2013): 59; Shan-Ying Chu, "Internet, Economic Growth and Recession," *Modern Economy,* no.4 (2013): 211.

[102] World Bank, GDP Growth (Annual %), (2016), http://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=GE.

[103] United Nations, Definition of Aggression, GA Resolution 29/3314 U.N. Doc. A/RES/29/3314 (December 14, 1974): Art. 3.

[104] IGE, *Tallinn Manual,* 505-507.

[105] Kaska, *International Cyber Incidents*, 74.

First, the coordination of the Georgia Attacks with Russian military operations was more than a seeming coincidence. The RBN rerouting of Georgian internet traffic to servers under its control, and DDoS attacks by RBN botnets, began on August 7th, a day before the general public was even aware that an armed conflict was erupting in Georgia.[106] Also, the Georgia Attacks appear to have been synchronized with Russian kinetic operations. For example, telecommunications targets in Gori were not engaged by Russian airstrikes as Russian ground forces advanced. Instead, those targets were neutralized by the Georgia Attacks.[107] This indicates the RBN had detailed knowledge of Russian military operations that could only have been obtained from Russian officials.

Second, the Georgia Attacks possessed a level of sophistication that indicates the involvement of Russian intelligence or military.[108] The reconnaissance of Georgian networks for infiltration routes, vulnerabilities, and target lists before Russian military operations also reveals prior knowledge of Russian intentions.[109] The Russian controlled servers involved in the Georgia Attacks, the cyber-attack kits used to facilitate the Georgia Attacks, and the campaign to weaponize cyber-rioters were also prepared well in advance of kinetic operations.

Third, some Russian officials have endorsed a policy of cyber-attacks by Russian hackers against other states.[110] Russia is also known to use cybercriminals as proxies for cyber-attacks that advance Russian national interests.[111] Given the level of RBN advanced knowledge of Russian operations, it is more likely than not that they conducted the Georgia Attacks under the effective control of Russian officials. This level of control would make the RBN a de facto agent of the state.[112]

Finally, Russia maintains tight control over internet access and the flow of data within its borders.[113] A copy of all public internet traffic is maintained by the Federal Security Service and the government controls all internet infrastructure.[114] Therefore, had the Russian government wished to stop the Georgia Attacks it could have easily done so. Instead, the Russians made no effort to stop the Georgia Attacks or even investigate after the fact. The activities of cybercriminal gangs like the RBN are both known to and condoned by the government because their services leverage Russian offensive cyber capabilities and create deniability.[115]

In total, the evidence supports a conclusion that it is more likely than not that Russia was responsible for the Georgia Attacks. To conclude that cyber-rioters spontaneously organized and launched the Georgia Attacks without substantial involvement by Russian officials is, at best, implausible. The advanced knowledge of the invasion and synchronization of the Georgia Attacks with Russian kinetic operations make coincidence a virtual impossibility. The ICJ, however, has established a clear and convincing standard of proof for the attribution of Article 2(4) uses of force.[116]

---

[106] Eneken Tikk, Kadri Kaska, & Liis Vihul, *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, November 2008), 4.

[107] Kozlowski, "Comparative Analysis," 240; Cornell, "Russia's War in Georgia," 18.

[108] Hagen, "The Russo-Georgian War," 15.

[109] Bumgarner, *Overview by the US-CCU*, 3; Krebs, "Russian Hacker Forums."

[110] Project Grey Goose, *Phase I Report: Russia/Georgia Cyber War – Findings and Analysis*, (October 17, 2008), 3.

[111] Brian Whitmore, "Organized Crime is Now a Major Element of Russian Statecraft," *Radio Free Europe Online,* October 27, 2015, http://www.businessinsider.com/organized-crime-is-now-a-major-element-of-russia-statecraft-2015-10; Matthew Dean & Catherine Herridge, "'Patriotic Hackers' Attacking on Behalf of Mother Russia," *Fox News Online,* January 16, 2016, http://www.foxnews.com/politics/2016/01/16/patriotic-hackers-attacking-on-behalf-mother-russia.html.

[112] Jason Healey, *"Beyond Attribution: Seeking National Responsibility for Cyber Attacks,"* The Atlantic Council, Cyber Statecraft Issue Brief, (January 2012): 3.

[113] Russell, *Cyber Blockades*, 112.

[114] Project Grey Goose, *Phase II Report: The Evolving State of Cyber Warfare*, (March 20, 2009), 23.

[115] Russell, *Cyber Blockades*, 119; Project Grey Goose, *Phase I Report*, 7; Keir Giles and Andrew Monaghan, *Legality in Cyberspace: An Adversary View* (Carlisle Barracks, PA: U.S. Army War College, March 2014), 19.

[116] *Oil Platforms* (Iran v. U.S.), 2003 I.C.J. 189-190 (November 6).

No such direct evidence of official Russian involvement is available, so the case for attribution of the Georgia Attacks to the Russian Government cannot be made with absolute confidence.

Military Character: The Georgia Attacks were closely synchronized with Russian kinetic operations. The manner in which the Georgia Attacks facilitated and supported Russian actions in the physical domains indicates they were a component of the campaign against Georgia.

When applied to the available evidence, the Schmitt Test does not support a conclusion that the Georgia Attacks violate Article 2(4) of the UN Charter. Additional research is needed to determine whether the effects of the cyber-blockade caused economic losses of sufficient severity. While the **Georgia Attacks clearly had a negative effect on Georgia's economy, it is impossible to determi**ne the degree of their impact absent empirical data. In addition, while substantial, the circumstantial **evidence of official Russian responsibility for the Georgia Attacks does not meet ICJ's standard of** proof for attribution. Additional direct evidence of state involvement is necessary to make the case. In the absence of a reliable measure of severity, and better confirmation of official Russian culpability, the evidence does not support concluding that the Georgia Attacks constituted a use of force under current international law.

Conclusion

The LOAC requires the world to rely on it for protection from acts of aggression, but it has not kept pace with the technological transformation of violence. Cyber-attacks can now inflict severe consequences on victim states without the application of kinetic force. Despite this fact, the UN **Charter's paradigm ties the hands of states in all but a very narrow category of cases.** The large unregulated space that most state sponsored cyber-attacks occupy encourages the very aggression the UN Charter was created to prevent. The Russo-Georgian War clearly illustrates this point, and subsequent cyber-attacks indicate that Russia continues to exploit this gap in international law to advance its national interests.

To address this challenge, the LOAC needs to be updated with a cyber-warfare convention. While the work of the GGE is a step in the right direction, participation by cyber offending states like Russia will continue to frustrate its efforts. The *Tallinn Manual* is another sign of progress, providing a solid foundation upon which to build. To address these complex issues, however, the U.S. and its allies must establish a forum tasked with producing a workable and effective treaty that regulates the use of force in cyberspace.
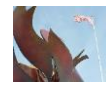
Strategic Robotpower: Artificial Intelligence and National Security

Patrick Sullivan

*Artificial intelligence (AI) will likely become **the central force in future society. AI's development** virtually guarantees that lethal autonomous weapons someday will be unleashed on the battlefield. Although these weapons could conceivably lower the human cost of war, they carry significant proliferation and collateral damage risks and could make the decision to go to war easier. This would be inherently destabilizing to the Westphalian geopolitical order, which is already under strain due to democratization of information. As the dominant artificial intelligence company, Google is best positioned to benefit from any decentralization and rebalancing of state power that occurs from AI-related disruption, with Silicon Valley as a whole becoming a political entity unto itself. Whatever the resultant decentralized/rebalanced power construct, all stakeholders— transnational technology companies, nation-states, and what remains of the international system—will have a responsibility to provide collective good **governance to ensure that AI's** outcomes are as positive as possible.*

Keywords: *Lethal Autonomous Weapons, Proliferation, Westphalian System, Google State*

Artificial intelligence (AI) promises to fundamentally change the way Americans live, work, and interact. In general, as technology grows more useful, demand grows. This principle will perhaps never be more true than with AI, given the rapid and dramatic progress it has ushered in disparate areas such as medicine, entertainment, finance, and defense.[1] AI and related technologies carry the promise of great and broad societal benefit. Given the close historical correlation between security and technological innovation, they also carry significant challenges for national security and

*Patrick J. Sullivan (M.S.S. United States Army War College) is a Lieutenant Colonel in the United States Army. An earlier version of this a**rticle, written under the direction of Dr. Andrew A. Hill, earned the prestigious Commandant's Award for** Distinction in Research for the USAWC class of 2017.*

[1] **Raffi Khatchadourian, "The Doomsday Invention,"** *The New Yorker Online*, November 23, 2015, http://www.newyorker.com/magazine/2015/11/23/doomsday-invention-artificial-intelligence-nick-bostrom.

policymaking.[2] The strategic impact of new technologies—usually measured in terms of disruption or destabilization—is difficult to predict.[3] Predicting the strategic impact of artificial intelligence is not just an issue of scale, however, but also of precedent: the very nature of AI demands that humanity consider its relationship with technology in entirely new ways.[4] Regardless of the difficulties and unknowns, this essay examines the implications of AI with respect to national security.

The methodology entails analyzing artificial intelligence within the four main themes of the 2015 *National Security Strategy of the United States* (NSS): defense of the United States and its allies, international order, values, and prosperity.[5] Although the Trump Administration published its own NSS outlining a fresh strategic vision for the United States, the four themes identified have remained fairly consistent since the first NSS in 1987, and due to their enduring nature constitute a valid analytical framework.[6]

Two core conclusions about artificial intelligence and national security become apparent from this analysis. First, future battlefields will prominently feature lethal autonomous weapons. Not only does this risk proliferation and catastrophic collateral damage, but it may also increase the frequency and intensity of armed conflict. Second, the manner in which AI technologies are developing and currently being used will likely cause state power to be rebalanced, with transnational technology companies such as Google best positioned to most benefit. As transnational influence takes hold, social inequality and related destabilization might increase such that existing institutions and policies may be exceedingly hard-pressed to mitigate the negative effects. In order for the resultant geopolitical, economic, and social orders to persist, a more agile governance structure will be needed. Placing these findings and their supporting analyses in proper context, however, requires a lexis for artificial intelligence as a scientific discipline, as well as a short history of its development.

Artificial Intelligence in Perspective

The term "artificial intelligence" was coined in 1956 by a summer research project at Dartmouth College, with foundations in Alan Turing's 1950 paper, "Computing Machinery and Intelligence," which proposed the famous Turing Test (AKA "The Imitation Game") to determine whether a machine could think.[7] Although no universally accepted contemporary definition for artificial intelligence exists, one of the discipline's founders, American computer scientist Nils J. Nilsson, provides a useful one: "Artificial intelligence is that activity devoted to making machines intelligent,

---

[2] Klaus Schwab, "The Fourth Industrial Revolution: What it Means and How to Respond," *World Economic Forum: Global Agenda Online*, January 14, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

[3] Adam Elkus, "The AI Wars?" *Slate: Future Tense – Citizen's Guide to the Future*, blog entry posted January 20, 2015, http://www.slate.com/articles/technology/future_tense/2015/01/what_artificial_intelligence_does_and_does_not_mean_for_security_and_geopolitics.html.

[4] Nayef Al-Rodhan, "The Security Implications and Existential Crossroads of Artificial Intelligence," *Georgetown Journal of International Affairs Online*, April 2, 2015, http://journal.georgetown.edu/the-security-implications-and-existential-crossroads-of-artificial-intelligence/.

[5] Barack Obama, *National Security Strategy* (Washington, DC: The White House, February 2015), 7-23. Also note that the first theme is actually "security" vice "defense," but I substituted defense to avoid confusion.

[6] All sixteen National Security Strategies (1987-2015) can be accessed at http://nssarchive.us/.

[7] Executive Office of the President, Committee on Technology, *Preparing for the Future of Artificial Intelligence* (Washington, DC: National Science and Technology Council), October 12, 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

and intelligence is that quality that enables an entity to function appropriately and with foresight in its environment."[8]

This definition correlates to modern conceptions of human intelligence, which is generally understood to be an efficient problem-solving ability that leverages past experience in a heuristic manner.[9] Comparing the definition of AI with this concept suggests that no machine is close to human-level intelligence, yet AI-enabled machines have outperformed master-level human competitors in chess, the TV game show *Jeopardy!*, and the ancient Chinese strategy board game "Go," all of which are abstract and highly complex.[10] To account for this seeming paradox, it is necessary to distinguish between narrow (or weak) AI and general (or strong) AI. The supercomputer victors of the games listed—IBM's Deep Blue, IBM's Watson, and Google DeepMind's AlphaGo—are each examples of narrow AI, which is specially designed to handle a very limited number of problem domains (usually one) through various forms of pattern recognition. A general AI on the other hand is not limited, and can ostensibly perform any intellectual task as well (but not necessarily in the same way) as a human.[11] In light of this distinction, all current AI applications such as targeted e-commerce and commercial services, natural language processing, image recognition and labeling, personal digital assistants (e.g., Apple's Siri or Amazon's Alexa), augmented medical diagnostic tools, and self-driving cars are narrow. These applications also represent an important bridge to a potential future general AI, as they have each resulted from a new wave of AI-related research that centers on machine learning.

In layperson terms, machine learning is the ability of computers to learn from data, as opposed to being explicitly programmed.[12] It does not represent a specific algorithm for singular problem-solving, but rather a general approach to solve many different problems.[13] Machine learning stems from cloud computing resources and Internet-based data gathering, both of which are recent innovations and whose commercial potential has radically exceeded initial expectations.[14] Coupled with new computing models such as artificial neural networks that replicate how the human brain functions, extreme data processing speeds enabled by advances in quantum mechanics, and evolutionary benchmarks such as machine vision and basic linguistic prediction, machine learning portends a near-term paradigm in which machines are capable of operating and adapting to changing real-world circumstances without human control.[15] At a minimum, such machine autonomy would

---

[8] Standing Committee of the One Hundred Year Study of Artificial Intelligence, *Artificial Intelligence and Life in 2030: Report of the 2015 Study Panel* (Stanford, CA: Stanford University, September 2016), https://ai100.stanford.edu/sites/default/files/ai_100_report_0831fnl.pdf. See also Nils J. Nilsson, *The Quest for Artificial Intelligence: A History of Ideas and Achievements* (Cambridge, UK: Cambridge University Press, 2010).

[9] Paul J. Springer, *Military Robots and Drones* (Santa Barbara, CA: ABC-CLIO, 2013), 33. Also consider "human-like" intelligence, to account for exceptionally "smart" animals such as dolphins, octopuses, and chimpanzees.

[10] Brent D. Sadler, "Fast Followers, Learning Machines, and the Third Offset Strategy," *Joint Force Quarterly Online 83* (October 1, 2016): http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-83/Article/969644/fast-followers-learning-machines-and-the-third-offset-strategy/. See also "Google's AlphaGo Beats Go Master Lee Se-Dol," *BBC: Technology News Online*, March 12, 2016, http://www.bbc.com/news/technology-35785875.

[11] Edward M. Lerner, "A Mind of Its Own, Part I: Artificial Intelligence," *Analog Science Fiction & Fact,* September 2016, 38-49.

[12] Chris Griffith, "Killer Robots," *The Australian Online*, November 3, 2016, http://www.theaustralian.com.au/life/personal-technology/killer-robots-are-closer-than-ever/news-story/74c20a6a186d9df3d5993da59c6475ad.

[13] Executive Office of the President, *Preparing for the Future of Artificial Intelligence.*

[14] Standing Committee, *Artificial Intelligence and Life in 2030.*

[15] Ibid. See also Randy Eshelman and Douglas Derrick, "Relying on the Kindness of Machines? The Security Threat of Artificial Agents," *Joint Force Quarterly Online* 77 (April 1, 2015): http://ndupress.ndu.edu/Media/News/News-Article-View/Article/581874/jfq-77-relying-on-the-kindness-of-machines-the-security-threat-of-artificial-ag/. See also John Markoff, "Microsoft Spends Big to Build a Computer out of Science Fiction," *New York Times Online*, November 20, 2016, https://www.nytimes.com/2016/11/21/technology/microsoft-spends-big-to-build-quantum-computer.html. See also

serve as a necessary condition for general artificial intelligence, which has been a core objective of AI research since the beginning.[16]

An additional concept commonly associated with general artificial intelligence is the technological singularity, **whereby a sufficiently "smart" and self**-aware machine could theoretically modify its own code recursively, producing new and more intelligent versions of itself in a chain reaction until a superintelligence emerged.[17] This superintelligence, by its very nature and method of creation, would, theoretically speaking, far surpass the ability of humans to understand and control, thus potentially posing an existential threat. Although the technological singularity has not occurred, and a malevolent-seeming superintelligence remains science fiction, the risk associated with development is increasingly subject to serious scientific and philosophical inquiry.[18] These inquiries are beyond the scope of this paper, however. In order to remain aligned with the analysis that follows, any negative implications of general artificial intelligence are manageable within the human condition and fall short of existential threat.

Despite the association with a potential superintelligence and the resultant "robot apocalypse," artificial intelligence is not about building a mind *per se*, rather it is about providing a gateway to expanded human potential through improved problem-solving tools.[19] In this context, the evolution from narrow to general AI is really just a shift from systems that have additive intelligent capabilities to ones that are sufficiently intelligent overall so that humans can better integrate with them.[20] Also, it bears remembering that artificial intelligence is still a nascent discipline and frontier science in comparison to technological history as a whole.[21] **Thus, while the various fears of AI's unknowns are** certainly valid, as related technologies become commonplace, they will no longer be seen as AI and even newer and more enigmatic technology will emerge.[22]

Through this continuous process of improvement and demonstrated utility, it is reasonable to expect that artificial intelligence will follow its current trajectory to become the central force in society with mostly positive impacts.[23] This is not guaranteed, however; the direction and effects of previous major technological shifts have not been consistently positive—which is an indictment of the technology itself as well as the supporting economic and policy landscape for a particular society.[24] This reality is disconcerting, as is the unprecedented pace of underlying change being driven by AI. The extraordinary complexity of artificial intelligence systems—which can make their performance unpredictable—and their development outside of the govern**ment's ability to** regulate **are two factors which aggravate the growing concern about AI's potentially** disruptive and

---

Gideon Lewis-**Kraus, "The Great A.I. Awakening,"** *The New York Times Magazine Online*, December 14, 2016, https://www.nytimes.com/2016/12/14/magazine/the-great-ai-awakening.html.

[16] Standing Committee, *Artificial Intelligence and Life in 2030.* See also Executive Office of the President, *Preparing for the Future of Artificial Intelligence.*

[17] Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (Oxford, UK: Oxford University Press, 2014).

[18] **In addition to Bostrom's work, see also James Barrat,** *Our Final Invention: Artificial Intelligence and the End of the Human Era* **(New York: St. Martin's Press, 2013); Nikola Danaylo**v, *Conversations with the Future: 21 Visions for the 21st Century* (Toronto: Singularity Media, Inc., 2016); George Zarkadakis, *In Our Own Image: Savior or Destroyer? The History and Future of Artificial Intelligence* (New York: Pegasus Books, 2016).

[19] Khat**chadourian, "The Doomsday Invention." See also Lewis**-Kraus, "The Great A.I. Awakening."

[20] Lewis-**Kraus, "The Great A.I. Awakening."**

[21] **Elkus, "The AI Wars?"**

[22] Standing Committee, *Artificial Intelligence and Life in 2030.*

[23] Ibid.

[24] Executive Office of the President, *Artificial Intelligence, Automation, and the Economy*, December 20, 2016, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Artificial-Intelligence-Automation-Economy.PDF.

destabilizing effects. These effects are inherent to national security and implicitly demand strong policy and strategy responses.

Killer Robots: AI and Defense

The history of military applications of artificial intelligence tacks closely to the history of the discipline itself. The Defense Advanced Research Projects Agency (DARPA) has conducted its own AI research for the better part of four decades, in addition to providing grant monies to academia and private industry through the Strategic Computing Initiative.[25] This research spawned AI-based navigation and sensing for explosive ordnance disposal robots and other unmanned ground systems, building upon earlier efforts to use ground robotics for remote control of vehicles and mounted weapons.[26] **RAND Corporation's Rule**-Oriented System for Implementing Expertise (ROSIE) was an early AI-based targeting tool that served as a precursor to AI systems now commonly used for target identification, discrimination, and recommendation in remotely-piloted aircraft (RPA), C-RAM (counter-rocket, artillery, and mortar) platforms, and the Aegis missile defense system.[27] Taken together with the increased importance of artificial intelligence in computerized war-gaming and **related decision aids, these applications show that military AI is moving away from exclusively "dull, dirty, and dangerous" tasks to ones that demand greater autonomy and complexity.**[28]

The appeal of AI-enabled autonomous weapons is practically self-evident. Autonomous weapons **could reduce "boots on the ground" requirements, enable greater precision in targeting, and increase** speed in decision-making, thereby lowering the human cost of war.[29] Additionally, autonomous weapons will likely be much cheaper to produce over time, since removing the operator allows miniaturization and simplifies systems integration.[30] This could help break the vicious defense acquisition cycle, in which the U.S. military seems to get less capability at greater expense generation-over-generation.[31] Moreover, Great Power competitors such as China and Russia are rapidly closing **the technological and doctrinal gaps that ensure the United States' current advantage in precision** strike and power projection, making reinvestment in these technologies both unaffordable and illogical in the long run.[32] The effectiveness of these technologies in a future operating environment increasingly characterized by hybrid warfare is debatable regardless, whereas artificial intelligence

---

[25] Springer, *Military Robots*, 34.

[26] P.W. Singer, *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (London: Penguin Press, 2009), 24-30.

[27] Jonas Stewart, *Strong Artificial Intelligence and National Security,* Final Report (Newport, RI: Naval War College Joint Military Operations Department, May 18, 2015), http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA622591. See also Jeffrey L. Caton, *Autonomous Weapon Systems: A Brief Survey of Developmental, Operational, Legal, and Ethical Issues,* The LeTort Papers (Carlisle Barracks, PA: U.S. Army War College, Strategic Studies Institute), http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=1309. See also Human Rights Watch, *Losing Humanity: The Case against Killer Robots,* (Washington, DC: Human Rights Watch, November 19, 2012), https://www.hrw.org/report/2012/11/19/losing-humanity-case-against-killer-robots.

[28] Paul Scharre, *Robotics on the Battlefield Part I: Range, Persistence, and Daring*, 20YY Series (Washington, DC: Center for a New American Security, May 2014), https://s3.amazonaws.com/files.cnas.org/documents/CNAS_RoboticsOnTheBattlefield_Scharre.pdf. See also United States Army, "U.S. Army Strategy for Robotic and Autonomous Systems (RAS)."

[29] Al-Rodhan, **"The Security Implications and Existential Crossroads."**

[30] **Arthur Herman, "The Pentagon's 'Smart' Revolution,"** *Commentary Magazine Online*, June 26, 2016, https://www.commentarymagazine.com/articles/pentagons-smart-revolution/.

[31] Ibid.

[32] Robert Martinage, *Toward a New Offset: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability* (Washington, DC: Center for Strategic and Budgetary Assessments, 2014), http://csbaonline.org/uploads/documents/Offset-Strategy-Web.pdf.

is, in the words of Deputy Secretary of Defense Robert O. Work, "The one thing that has the widest application to the widest number of Department of Defense (DOD) missions" moving forward.[33] Russia's Chief of General Staff and one of the intellectual fathers of hybrid warfare, General Valery Gerasimov, endorses this view, predicting a future battlefield dominated by learning machines.[34] Additionally, numerous AI researchers have forecasted autonomous weapons as the third military-technical revolution, after gunpowder and nuclear weapons.[35]

Although autonomous weapons tend to get associated with the more extreme elements of science fiction, such as the "killer robots" of the Terminator franchise, mobile general artificial intelligence (a more precise name for a robot) is not necessary to develop an autonomous weapon; much of the foundational technology exists today and several precursor systems are already in use.[36] These include the Samsung SGR-A1 Sentry Gun in the Demilitarized Zone on the Korean Peninsula, and the Israeli Defense Force's SentryTech system, both of which have settings that allow for lethal engagement without human intervention.[37] Even the C-RAM systems used by the U.S. military are *de facto* autonomous with lethal potential, at least collaterally; although a human operator supervises the system, he or she would have to react near-instantaneously to override an engagement.[38]

Although no nations have fully committed to the development of AI-enabled autonomous weapons, none have disavowed them either.[39] For the United States, the current trend is towards development. The U.S. Army Strategy for Robotics and Autonomous Systems envisions autonomous systems incorporated into combined arms maneuver by 2035, with dynamic force and mission autonomy to follow in the 2040s.[40] DARPA initiated a program in 2013 to integrate machine learning in a wide variety of weapon systems, and the Office of Naval Research is funding several studies in support of its broader vision to "develop autonomous control that intelligently understands and reasons about its environment … and independently takes appropriate action."[41] From a U.S. policy perspective, DOD Directive 3000.09, *Autonomy in Weapon Systems*, calls for the identification of operational needs that can be satisfied by autonomous weapon systems while neither encouraging nor prohibiting these systems having lethal capabilities.[42] Exploiting the space created by this opacity, the U.S. Army's last research and development budget submission outright describes lethal ground autonomous weapons.[43]

---

[33] Matthew Rosenberg and John Markoff, "At Heart of US Strategy, Weapons That Can Think," *New York Times Online*, October 26, 2016, http://www.nytimes.com/images/2016/10/26/nytfrontpage/scannat.pdf.

[34] Sadler, "Fast Followers."

[35] Future of Life Institute, "Autonomous Weapons: An Open Letter from AI & Robotics Researchers," https://futureoflife.org/open-letter-autonomous-weapons/.

[36] Scharre, *Robotics on the Battlefield Part I.*

[37] Brad Allenby, "What is 'Military Artificial Intelligence'?" *Slate: Future Tense – Citizen's Guide to the Future*, blog entry posted December 2, 2016, http://www.slate.com/articles/technology/future_tense/2016/12/the_difficulty_of_defining_military_artificial_intelligence.html. See also Human Rights Watch, *Losing Humanity.*

[38] Human Rights Watch, *Losing Humanity.*

[39] Paul Scharre, *Autonomous Weapons and Operational Risk,* Ethical Autonomy Project (Washington, DC: Center for a New American Security: February 2016), https://s3.amazonaws.com/files.cnas.org/documents/CNAS_Autonomous-weapons-operational-risk.pdf.

[40] U.S. Department of the Army, "U.S. Army Strategy for Robotic and Autonomous Systems (RAS)."

[41] Al-Rodhan, "The Security Implications and Existential Crossroads." See also Caton, *Autonomous Weapon Systems: A Brief Survey.*

[42] Caton, *Autonomous Weapon Systems: A Brief Survey.* See also Executive Office of the President, *Preparing for the Future of Artificial Intelligence.*

[43] Program Element 0603827A, Soldier Systems-Advanced Development, Project S54, Small Arms Improvement. See Caton, *Autonomous Weapon Systems: A Brief Survey.*

The DOD Directive 3000.09 is a bit clearer on the control of autonomous weapon systems, saying they must employ "appropriate levels of human judgement."[44] In the near term at least, this is understood to mean that a human operator will always be in-the-loop (the human controls the weapon) or on-the-loop (the human supervises the weapon and can override it if necessary).[45] This includes manned-unmanned teaming concepts favored by "centaur warfighting" and the DOD's "Third Offset" acquisition strategy, which relies heavily on artificial intelligence technologies.[46] Additionally, as autonomous weapons development gains momentum, concomitant concerns over independence and lethality are assuaged somewhat by the belief that the systems will be defensive in nature, similar to the quasi-autonomous sentries already in use. This is false comfort, however. As Paul Scharre, Director of the Future of Warfare Initiative at the Center of a New American Security, has observed, "if there was an easy way to delineate between offensive and defensive weapons, nations would have agreed long ago to only build 'defensive' weapons."[47]

Commitments to keeping humans in or on-the-loop are not sufficient to allay concerns about ceding control of lethal decisions to a machine, or to avoid creating potentially uncontrolled killer robots. On the contrary, numerous incentives make the development of lethal autonomous weapons borderline inevitable as long as artificial intelligence continues to deliver on its technological promise. Although AI-enabled machines are not yet as "smart" as humans, they are far superior at solving multiple control problems very quickly, due to their ability to process massive amounts of information to detect patterns without suffering fatigue, recognition error, bias, or emotional interference.[48] At the tactical level, military operations are basically just a series of control problems, and decision-making in competitive environments tends to accelerate; this is what Sun Tzu was suggesting when he described speed as "the essence of war."[49] Thus, a human operator in or on-the-loop detracts from the very advantage that autonomous weapons and other military AI applications provide.[50] Add to this the fragility of communication links in a hybrid operating environment with cyber and anti-access elements, and the operational imperative to delegate actions—including lethal ones—directly to machines becomes clear.[51]

The "first mover" principle is also at play. Militaries have an intrinsic motivation to develop superior capabilities to their adversaries. The first competitor to maximize AI's potential to fundamentally change the character of future warfare would enjoy a significant tactical and operational advantage.[52] The United States is already at the forefront for AI technologies, has a defense industrial base that leads the world in complex systems engineering and integration, and has

---

[44] Ashton Carter, *Autonomy in Weapon Systems,* Department of Defense Directive 3000.09 (Washington, DC: U.S. Department of Defense, November 21, 2012), http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf.

[45] Ibid.

[46] Martinage, *Toward a New Offset.* See also Scharre, *Robotics on the Battlefield Part I*. See also Paul Scharre, "Robotics on the Battlefield Part II: The Coming Swarm," *Center for a New American Security: 20YY Series*, October 2014, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_TheComingSwarm_Scharre.pdf.

[47] John Markoff, "Pentagon Turns to Silicon Valley for Edge in Artificial Intelligence," *New York Times Online*, May 11, 2016, https://www.nytimes.com/2016/05/12/technology/artificial-intelligence-as-the-pentagons-latest-weapon.html.

[48] Kareem Ayoub and Kenneth Payne, "Strategy in the Age of Artificial Intelligence," *Journal of Strategic Studies Online* 39, (November 2015), http://www.tandfonline.com/doi/pdf/10.1080/01402390.2015.1088838?needAccess=true.

[49] Scharre, *Robotics on the Battlefield Part I.* See also Scharre, "Autonomous Weapons and Operational Risk." See also Sun Tzu, *The Art of War* (Sweden: Chiron Academic Press, 2015).

[50] Stewart, *Strong Artificial Intelligence and National Security.*

[51] Robert O. Work and Shawn Brimley, "20YY: Preparing for War in the Robotic Age," *Center for a New American Security: 20YY Series*, January 2014, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_20YY_WorkBrimley.pdf.

[52] Sadler, "Fast Followers." See also Herman, "The Pentagon's 'Smart' Revolution."

tremendous practical experience with RPAs and unmanned ground vehicles from which to draw.[53] Accordingly, the U.S. is in the best position to be the first mover for lethal autonomous weapons and to gain tactical and operational advantages.

Regardless of how the United States sees its first mover advantage, the development of lethal autonomous weapons is highly probable due to factors beyond U.S. control. Most artificial intelligence and machine learning research is occurring openly in the private sector and academia, untethered to military contracts and generally without an eye towards military applications (no matter how obvious these applications may be). Even technologies developed at DARPA typically do not remain classified.[54] Moreover, a formal ban under the auspices of the Convention on Certain Conventional Weapons or similar agreement is unlikely, since restrictions of this form usually have disproportionate impact on states that most rely on the technologies related to the weapon, i.e., the United States and China in this case.[55] Thus, Great Power competitors will have access to the foundational AI technologies for lethal autonomous weapons, and given the incentives already described, will likely seek to develop new and dangerous concepts of operation that leverage them.[56] Accordingly, using its first mover advantage to define the probable shift to lethal autonomous weapons is arguably the most responsible and stabilizing choice the United States can make.

Once this change is fully defined, irrespective of origin, it will trigger a military imperative to adapt to it. This includes proactively dealing with the foreseeable consequences, of which proliferation and system unpredictability are the most alarming. Regarding proliferation, it is almost certain that rogue states and/or violent extremist organizations would either design their own non-discriminatory lethal autonomous weapons, or remove safeguards from a system already developed by a more responsible actor.[57] History is replete with unsuccessful attempts to control technology once loosed—gunpowder and submarines are both prominent examples.[58] Many artificial intelligence researchers fear that the technological trajectory of autonomous weapons is such that they **"will become the Kalashnikovs of tomorrow," with particular utility in assassinations, ethnic** cleansing, destabilizing governments, and population control.[59] Absent an unlikely ban on lethal autonomous weapons, or even more unlikely suppression of the foundational AI technologies, proliferation risk simply becomes manageable.[60]

Unpredictable performance of lethal autonomous weapons can create accidental and collateral damage risk that would also have to be managed. Anthropomorphizing machines is human nature, but artificial intelligence and cascading technologies are functionally different than any form of human cognition, and will thus act in ways not anticipated by developers.[61] In fact, this is part and parcel with the whole concept of autonomy.[62] For machine learning, an AI system is trained on inputs and outputs, often unsupervised, until *voilà!* It just works. In this fashion, machine learning is akin

---

[53] Martinage, *Toward a New Offset.*

[54] Rosenberg and Markoff**, "At Heart of US Strategy." See also Christopher Mims, "We're Fighting Killer Robots the Wrong Way,"** *The Wall Street Journal Online,* August 17, 2015, https://www.wsj.com/articles/were-fighting-killer-robots-the-wrong-way-1439784149.

[55] Allenby, "What is 'Military Artificial Intelligence'?"

[56] Mims, "We're Fighting Killer Robots the Wrong Way."

[57] Herman, "The Pentagon's 'Smart' Revolution." See also Griffith, "Killer Robots."

[58] Eshelman and Derrick, "Relying on the Kindness of Machines?"

[59] Future of Life Institute, "Autonomous Weapons: An Open Letter."

[60] Edward M. Lerner, "A Mind of Its Own, Part II: Superintelligence," *Analog Science Fiction & Fact,* October 2016, 25-35.

[61] Ayoub and Payne, "Strategy in the Age of Artificial Intelligence."

[62] Human Rights Watch, *Losing Humanity*. See also Eshelman and Derrick, "Relying on the Kindness of Machines?"

to a "black box," with developers sacrificing understanding of AI system behavior and shortchanging control in favor of performance.[63] Artificial neural networks in particular can sometimes yield odd and unpredictable results, and if an artificial intelligence is based on quantum computer modeling, then the AI itself will embody quantum indeterminacy.[64] Additionally, an autonomous AI in a physical environment is subject to the "open world" conundrum, in which the system is bound to encounter conditions that were not anticipated when it was designed and built.[65]

Thus, lethal autonomous weapons will inevitably produce errors, and not necessarily ones a human operator would produce if they were in or on-the-loop.[66] These errors will be difficult to correct or prevent from reoccurring; not only could the sheer complexity of the weapon system prevent an error's cause from being auditable, it is difficult to take corrective action without understanding how the weapon system is behaving and why.[67] Also, automation bias – through which humans demonstrate uncritical trust in automation and its outputs – could create denial that an error has even occurred.[68]

The negative outcomes of the accidental and collateral damage risk accrued with a lethal autonomous weapon's error production are fratricide and civilian casualties. Although AI-related error can reasonably be expected to occur much less frequently than human error, lethal autonomous weapons have higher damage potential over possibly orders of magnitude more social-technological interactions, some of which will have not been anticipated by the system's designers.[69] Moreover, one has to take any artificial intelligence on interface value, so a lethal autonomous weapon's error would likely repeat with a consistent level of force until some external agent intervened.[70] Human error, on the other hand, tends to be idiosyncratic and one-off given a human operator's (presumed) common sense, moral agency, and capacity for near-real time consequence management.[71]

Unjust War – AI and International Order

In addition to altering the tactical and operational environments, the lethal autonomous weapons paradigm and other military artificial intelligence applications pose strategic risk. Not only will artificial intelligence potentially change the criteria for war and how it is conducted, but it might also fundamentally disrupt the geopolitical landscape in which war is waged.

Although AI can potentially reduce the human cost of war within individual conflicts, this reduction could make conflicts themselves occur more frequently and with greater intensity.[72] The

---

[63] Luke Dormehl, "Algorithms: AI's Creepy Control Must Be Open to Inspection," *The Guardian Online*, January 1, 2017, https://www.theguardian.com/commentisfree/2017/jan/01/algorithms-ai-artificial-intelligence-facebook-accountability. See also Lerner, "A Mind of Its Own, Part II," 25-35.

[64] Scharre, *Autonomous Weapons and Operational Risk.* See also Lerner, "A Mind of Its Own, Part I," 38-49.

[65] Executive Office of the President, *Preparing for the Future of Artificial Intelligence.*

[66] The AI Now Report, "The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term," Summary of the AI Now Public Symposium, Hosted By the White House and New York University's Information Law Institute, July 7, 2016, https://artificialintelligencenow.com/media/documents/AINowSummaryReport_3.pdf.

[67] Executive Office of the President, National Science and Technology Council, *The National Artificial Intelligence Research and Development Strategic Plan,* Report of the Network and Information Technology Research and Development Subcommittee (Washington, DC: The White House, October 13, 2016), https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf.

[68] Scharre, *Autonomous Weapons and Operational Risk.*

[69] Ibid.

[70] Dormehl, "Algorithms: AI's Creepy Control."

[71] Scharre, *Autonomous Weapons and Operational Risk.*

[72] Stewart, *Strong Artificial Intelligence and National Security.* See also Schwab, "The Fourth Industrial Revolution."

human cost of war is an important consideration in the decision to use violent force; in fact, the principle of *jus ad bellum* (literally "justice of war," i.e., the conditions under which a state can rightly or justly resort to the use of force) is often predicated on this calculation.[73] If the potential for casualties is minimal, then governments might be inclined to operate with less restraint in using the military instrument to secure national interests.[74] The way in which the United States brazenly challenges other nations' sovereignty with the use of armed remotely piloted aircraft (RPA) is an indication of diminished restraint. Also, the 2015 National Security Strategy commits to "avoiding costly large-scale ground wars," but underwrites the use of proxies and asymmetric methods to combat violent extremist organizations, thereby lowering the threshold for war.[75] This latter point and recent history suggest that the United States and its partners have a troubling predilection for the "Jupiter Complex" – using force to exact righteous retribution against perceived evil adversaries. Artificial intelligence could potentially create a positive feedback loop encouraging this behavior.[76]

The human cost of war would likely normalize over time with the proliferation of lethal autonomous weapons, but if certain populations had developed a sense of invulnerability in the interim, they would be less prepared for the burdens of war moving forward.[77] Accordingly, policy-makers would need to be careful that military AI applications do not become a detriment to the population's sense of national identity and collective purpose. Policy-makers should be further cautioned that, despite the appeal and apparent low cost of AI-enabled warfare, any military engagement is inherently destabilizing.[78] For the lethal autonomous weapons paradigm, at least at the outset, the destabilizing effects center on a potential availability gap for foundational AI technologies. An availability gap could reinforce and exacerbate global inequalities, as well as incentivize a "first strike" or new forms of extremism to close the gap.[79] In response, the AI-advantaged nation's basic assumptions of deterrence and compellence would be severely challenged, thus changing the tenets of their defense strategy.[80]

Lethal autonomous weapons in particular also represent a responsibility gap that goes beyond the accidental and collateral risks associated with errors and system failures.[81] It is doubtful that an artificial intelligence with lethal capacity could uphold the two central elements of *jus in bello* ("justice in war," or the law that governs how force is to be used), namely discrimination and proportionality. Regarding discrimination, restricting the use of lethal autonomous weapons to a self-regulated set of narrowly constructed scenarios is difficult since the system's developers would not be able to anticipate every interaction the system might encounter.[82] The system's inherent "framing problem," in which it would inevitably have incomplete understanding of its external environment, just adds to its intractability.[83] The developer could attempt to install a sense of compassion, empathy, and mercy in the system, but installed ethics are liable to become obsolete due

---

[73] Human Rights Watch, *Losing Humanity.* See also Sadler, "Fast Followers."

[74] Al-Rodhan, "The Security Implications and Existential Crossroads." See also Caton, "Autonomous Weapon Systems: A Brief Survey."

[75] Obama, *National Security Strategy*, 7-10. See also Human Rights Watch, *Losing Humanity.*

[76] Caton, "Autonomous Weapon Systems: A Brief Survey."

[77] Scharre, *Robotics on the Battlefield Part II.*

[78] Al-Rodhan, "The Security Implications and Existential Crossroads."

[79] Ayoub and Payne, "Strategy in the Age of Artificial Intelligence." See also Al-Rodhan, "The Security Implications and Existential Crossroads."

[80] Work and Brimley, *20YY: Preparing for War in the Robotic Age.*

[81] Human Rights Watch, *Losing Humanity.*

[82] Human Rights Watch, *Mind the Gap: The Lack of Accountability for Killer Robots* (Washington, DC: Human Rights Watch, April 9, 2015), https://www.hrw.org/report/2015/04/09/mind-gap-lack-accountability-killer-robots.

[83] Human Rights Watch, *Losing Humanity.*

to similar issues of framing and unanticipated interactions.[84] Thus, since the lethal autonomous weapon will likely not possess the equivalence of moral agency or social norming—to reiterate, there is nothing inherently human about a machine—it will ruthlessly and relentlessly carry out **assignments, with none of Clausewitz's fog or friction to temper its actions.**[85] The lack of moral agency precludes a lethal autonomous weapon from being held accountable, since it cannot fear nor learn from punishment.[86]

A machine's capacity for proportionality fails along a similar line of argument. Although a lethal autonomous weapon's lack of emotion checks the passions of war, which can lead to atrocities and revenge killings, it also constrains prediction of an adversary's emotions and actions.[87] Proportionality requires judgment and depends greatly on context which, given its framing problem, a lethal autonomous weapon is unlikely to be able to process.[88]

Artificial intelligence and lethal autonomous weapons could also complicate efforts to stabilize crises.[89] Crisis settings often demand quick decisions with incomplete information; if an ill-considered decision creates an unanticipated lethal autonomous weapon interaction with an error or **failure outcome, then an unintended "flash war" could result.**[90] Although this type of conflict could start quickly, there is no guarantee that it would end quickly. On the contrary, given the rapid and high volume interactions of complex autonomous systems, the flash war would conceivably spiral out of human control and be difficult to stop.[91] The ensuing chaos would support the interests of rogue states, violent extremist organizations, and practitioners of hybrid warfare. Accordingly, these groups could be expected to create conditions for flash wars through use of lethal autonomous weapons, or by hacking fail-**safes in someone else's weapon if the intent is to avoid attribution.**[92]

The flash war scenario suggests a forthcoming geopolitical environment in which artificial intelligence allows military power to be decoupled from traditional indices such as population size/growth and gross domestic product.[93] This decoupling could fundamentally change the character of alliances and security cooperation agreements, since apparently weak states would no longer need the protection of ostensibly strong ones. Alliances would also potentially no longer be influenced by forward basing and access considerations, since AI-enabled additive manufacturing, small high-density power generation, and miniaturization will likely change power projection modalities.[94] Adam Elkus, a Cybersecurity Fellow at the public policy think tank New America, **describes this course as, "[artificial] intelligence creating a new form of meta**-geopolitics that will **reshape notions of national power."**[95] Within this new form meta-geopolitics, proliferation of lethal

---

[84] Lerner, "A Mind of Its Own, Part I," 38-49. See also **Ayoub and Payne, "Strategy in the Age of Artificial Intelligence."** See also Executive Office of the President, *The National Artificial Intelligence Research and Development Strategic Plan.*

[85] **Ayoub and Payne, "Strategy in the Age of Artificial Intelligence."** See also **Al-Rodhan, "The Security Implications and Existential Crossroads."**

[86] Human Rights Watch, *Mind the Gap.*

[87] Human Rights Watch, *Losing Humanity.* See also **Sadler, "Fast Followers."**

[88] Human Rights Watch, *Losing Humanity.*

[89] Ayoub and P**ayne, "Strategy in the Age of Artificial Intelligence."** See also Work and Brimley, *20YY: Preparing for War in the Robotic Age.*

[90] **Scharre, "Autonomous Weapons and Operational Risk."**

[91] Scharre, *Robotics on the Battlefield Part I.*

[92] **Scharre, "Autonomous Weapons and Operational Risk."**

[93] Work and Brimley, *20YY: Preparing for War in the Robotic Age.* See also Herman, "The Pentagon's 'Smart' Revolution." **See also** Scharre, *Robotics on the Battlefield Part I.*

[94] Work and Brimley, *20YY: Preparing for War in the Robotic Age***. See also** Herman, "The Pentagon's 'Smart' Revolution."

[95] **Elkus, "The AI Wars?"**

autonomous weapons could democratize violence, providing individuals and groups with state-level instruments of military power.[96] Different AI technologies will democratize information by providing smaller entities with state-level instruments of softer types of power.

Artificial intelligence is promoting technological growth and diffusion of knowledge at unprecedented rates, and its transformative effects on society seem to be accelerating.[97] With this diffusion of knowledge, human and strategic interests are merging, sometimes forcefully so.[98] Evidence abounds for this rise in human agency, from the hacktivist collective Anonymous' use of AI programs to support the Arab Spring, to AI-enabled social media fueling demands for social justice across the world, to social impact investing and entrepreneurship spawning what Nicholas Kristof of the *New York Times* has called "DIY foreign aid."[99] Previously dormant socio-economic, cultural, and ethnic fault lines are fracturing, and state power is proving increasingly inadequate to tamp down unleashed conflicts, assuming that the state is even paying attention to the disruptive forces.

The inability of state power to manage AI-related disruption has invited questions about the future suitability of the Westphalian system of nation-state sovereignty. Although predictions about the return of the city-state or the rise of a "new medievalism" are probably oversold, it is clear at a minimum that human agency is forcing the redistribution and decentralization of power to non-state actors.[100] Given the deep interconnection of commerce and geopolitics that already exists with globalization, foremost among these non-state actors are transnational corporations, some of which are as powerful as nation-states yet beholden to none.[101] Given the outsized influenced of artificial intelligence on the approaching social and economic orders, the most consequential transnational corporations and, by extension, the most powerful non-state actors will be technology companies.

Rise of the Google State: AI, Prosperity, and Values

The proverbial alpha in the technology company pecking order will likely be Google. Google is all-in with machine learning, employing the largest number of Ph.D.s in the field—outstripping even academia—and their "AI First" growth strategy envisions the widening industrial applications of self-programming computers.[102] These applications could potentially transform the basis of economic growth for countries throughout the world, and Google is well-positioned to dominate this new economic order in ways that go far beyond its talent advantage.

"AI First" represents what some observers have described as "institution building and consolidation of power on a scale and at a pace unprecedented in human history."[103] Google has unmatched reserves of data in a massive cloud and supercomputing architecture that spans 13

---

[96] Herman, "The Pentagon's 'Smart' Revolution." See also Schwab, "The Fourth Industrial Revolution." See also Scharre, *Robotics on the Battlefield Part I.*

[97] Eshelman and Derrick, "Relying on the Kindness of Machines?" See also Schwab, "The Fourth Industrial Revolution." See also Brad Stone, "Silicon Valley Reckons with its Political Power," *Bloomberg Online*, December 22, 2016, https://www.bloomberg.com/news/articles/2016-12-22/silicon-valley-reckons-with-its-political-power.

[98] Al-Rodhan, "The Security Implications and Existential Crossroads."

[99] Anne-Marie Slaughter, "The Only Way Forward: Can the New World Order Be Saved By Humanism?" *Foreign Policy Online Global Thinkers 2016*, https://gt.foreignpolicy.com/2016/essay/the-only-way-forward?df8f7f5682. See also Al-Rodhan, "The Security Implications and Existential Crossroads."

[100] Michael Vaughan, "After Westphalia, Whither the Nation State, Its People, and Its Governmental Institutions?" September 29, 2011, https://espace.library.uq.edu.au/data/UQ_266787/AfterWestphalia.pdf.

[101] "Is History's Most Ruthless Company the Future of Business?" *Slate Online*, December, 2016, http://www.slate.com/articles/arts/taboo/2016/12/taboo_east_india_company_circa_2016.html. See also Vaughan, "After Westphalia."

[102] Khatchadourian, "The Doomsday Invention." See also Lewis-Kraus, "The Great A.I. Awakening."

[103] Lewis-Kraus, "The Great A.I. Awakening."

countries distributed over four continents, which provides them a distinct strategic advantage over technology company competitors.[104] This is because the company that possesses the data controls the algorithms for continued machine learning research and physical system integration. Eric **Schmidt, CEO of Alphabet, Google's parent company, has predicted that big data will be the "new oil"** – a commodity so consequential in the global economic order that nations will fight over it.[105] And **given Google's existing computing architecture, their data reserves are likely to increase outside of their core business model, since smaller companies will be more inclined to tap into Google's cloud** resources as opposed to investing the billions of dollars to build their own secure architecture.[106]

With Google's incumbent control of big data, it will be able to use artificial intelligence to refine its products better than any potential competitor or market entrant, thereby ensuring its dominance until the market fundamentally changes or some successor paradigm forces a new global economic order.[107] Such a change is unlikely in the foreseeable future. On the contrary, it is more likely that Google and its transnational technology company brethren in Silicon Valley will dominate much more than the economic order.[108] On September 12, 2016, for the first time in history, the five largest public corporations by market capitalization were technology companies, each of which are heavily invested in AI.[109] Greater awareness of their collective power will increasingly force Silicon Valley companies to act in their own self-interest (as any transnational company should be expected to), and the resources and influence that these companies command will ensure that their actions are politically significant, regardless of intent. In this manner, technology will continue to become a sort of political entity unto itself, with technology companies not realistically having the option to stay neutral in the public policy space, with either their products or their stated positions.[110]

If AI-enabled social media platforms and search engines do not remain politically neutral, then the democratic process can suffer greatly as a result, therein comprising yet another disruption vector for AI into the national security setting. Predictive algorithms could greatly improve the reach and effectiveness of robo-calls, social media bots, and gerrymandering of voting districts, which would suppress democratic participation and increase fractiousness in the increasingly polarized political environment.[111] **Artificial intelligence already acts as an "invisible authority" on the Internet that** reflects back its image of consumers. The pervasiveness of AI applications to help organize a highly complex world renders society amenable to relinquishing control.[112] **Hence consumers' willingness** to give up much of their privacy to Google and others (to include governmental entities, tacitly or transitively) to facilitate the passive collection of the data necessary for machine learning AI applications to work and further improve.[113] Thus, the stage is set for technology companies to serve

---

[104] Ibid.

[105] Rob Price, "Alphabet's Eric Schmidt: Big Data is So Powerful, Nation States Will Fight Over It," *Business Insider Online*, March 9, 2017, http://www.businessinsider.com/google-eric-schmidt-countries-will-fight-over-big-data-alphabet-cloud-2017-3.

[106] Ibid.

[107] Executive Office of the President, *Artificial Intelligence, Automation, and the Economy.*

[108] President Trump, for example, was elected over the near-universal objection of Silicon Valley, and that several prominent Silicon Valley executives and inve**stors have led the call for California's secession from the United States.** Stone, "Silicon Valley Reckons With Its Political Power."

[109] Ibid.

[110] Vaughan, "After Westphalia." See also Dormehl, "Algorithms: AI's Creepy Control."

[111] Standing Committee, *Artificial Intelligence and Life in 2030.* See also Sydney Finkelstein, "Algorithms are Making Us Small-**Minded,"** *BBC Online*, December 12, 2016, http://www.bbc.com/capital/story/20161212-algorithms-are-making-us-small-minded.

[112] Dormehl, "Algorithms: AI's Creepy Control."

[113] Stone, "Silicon Valley Reckons With Its Political Power."

as "Big Brother," controlling ideas to potentially nefarious ends, and along the way reducing the sociability and consciousness that make us all "human."[114]

As it stands, AI-enabled social media is not used as tool to bring people together but rather to sow division, particularly among groups who are already feeling left behind by the emerging global economic order. Prominent among these groups are workers most susceptible to job displacement that is being caused by AI-driven automation, and for whom Silicon Valley has become an agent of destruction.[115]

More jobs have been lost to technology in the United States over the last decade than any other sector, and this development is likely to accelerate as automation costs come down and AI technologies gain even greater primacy in all facets of the economy.[116] Due to the nature of automation *vis-à-vis* current narrow AI capabilities, the jobs lost and threatened are highly concentrated among lower skilled and less educated workers. According to a study completed by former President Obama's National Science and Technology Council, between nine and 47 percent of all American jobs are at risk of displacement over the next two decades and 83 percent of these jobs are concentrated in the lower middle class.[117] This continues a trend since the latter half of the 20th Century of increasing system bias towards skilled labor, as well as production's increasing reliance on capital at the expense of labor as a whole.[118] For workers who have already been displaced, their demonstrated difficulty in matching extant skills to the AI economy's in-demand jobs indicates the long-term disruptive potential of job displacement, with certain parts of the workforce moving toward permanent unemployment and poverty.[119]

In-demand jobs are at the very high-end or very low-end of the pay scale. The resultant "hollowing out" of the middle class will increasingly bifurcate the job market between the two extremes of low-skill/low-pay and high-skill/high-pay, thereby increasing social tensions and promoting a belief that capitalism's "winner take all" ethos is not working for most.[120] Since many people derive a significant amount of meaning, identity, and self-worth from their employment, the potential for malaise and its negative effects—crime, social dereliction, etc.—become clear.[121]

The inequalities created by the AI economy are potentially far greater and more disruptive than those related to mere job displacement. Additional segregation could occur exclusively in the high end of the skill and pay scales. In an economy where machines are doing most of the work, virtually all of a company's returns would go to investment as opposed to labor.[122] This in turn would create a premium for intellectual capital – those select few from the uppermost stratum who can direct the ever increasing resources in the most profitable and visionary ways: the same Silicon Valley titans who are currently shaping and setting the AI economy. Additionally, forecasting the jobs that will be

---

[114] Slaughter, "The Only Way Forward." See also Standing Committee, *Artificial Intelligence and Life in 2030.* See also Schwab, "The Fourth Industrial Revolution."

[115] Stone, "Silicon Valley Reckons With Its Political Power."

[116] Martinne Geller and Ben Hirschler, "Impact of Job-Stealing a Growing Concern at Davos," *Reuters Online*, January 20, 2017, http://www.reuters.com/article/us-davos-meeting-robots-idUSKBN1540HO.

[117] Executive Office of the President, *Artificial Intelligence, Automation, and the Economy.*

[118] Executive Office of the President, *Artificial Intelligence, Automation, and the Economy.* See also Standing Committee, *Artificial Intelligence and Life in 2030.* See also Schwab, "The Fourth Industrial Revolution."

[119] Executive Office of the President, *Artificial Intelligence, Automation, and the Economy.* See also Cade Metz, "The AI Threat Isn't Skynet. It's the End of the Middle Class," *Wired Business Online*, February 10, 2017, https://www.wired.com/2017/02/ai-threat-isnt-skynet-end-middle-class/. See also The AI Now Report, "The Social and Economic Implications of Artificial Intelligence."

[120] Schwab, "The Fourth Industrial Revolution." See also Metz, "The AI Threat Isn't Skynet."

[121] Ibid.

[122] Schwab, "The Fourth Industrial Revolution."

lost to or threatened by artificial intelligence is easier than predicting what jobs will be in demand and how much production will actually rely on them.[123] Thus, the AI economy could actually **represent "superstar biased" technological change, in which labor becomes virtually non**-existent (or *de facto* irrelevant from a policy perspective), thereby fundamentally changing the nature of production and work.[124] Accordingly, economies would have to be reorganized to enable a new form of resource allocation other than compensation for labor.[125] And as Silicon Valley is best positioned to benefit from the AI economy, its political weight will likely prove decisive in dictating what that reorganization will be.

Conclusion: Governance is Destiny

Social upheaval, political turmoil, privacy concerns, and good old class warfare are reasons many prognosticators suggest as to why societies have nothing to fear from killer robots or the like. People will rise up well before machines do.[126] No matter when or in what context AI-induced disruption occurs, however, it will engender national security concerns. Given disruption already exists despite the relatively immature status of artificial intelligence technologies at present, disruption will likely get worse before it gets better. In turn, the national security setting will likely be much less stable in the interim.

Artificial intelligence is here to stay, and will continue to gain influence and utility. It will one day become the central force in society, for good and for ill. Although the national security implications of AI are consequential and potentially severe, one can nonetheless believe that the benefits of AI will outweigh the costs. Recognition that technology is not destiny helps. Technological advancements have occurred throughout history, with various economies experiencing qualitatively different outcomes because of different policies and institutions.[127] Indeed, the critical factor that will shape the future of AI is the same factor that shapes the AI present: governance. What constitutes governance will likely change with the decentralization and rebalancing of state power. Regardless of where the power lies—within nation-states, within Silicon Valley, and/or within what remains of the international system—there will be a set of strategic leaders to wield it. May they demonstrate the intelligence, artificial and human, to do so responsibly.
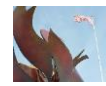
---

[123] Standing Committee, *Artificial Intelligence and Life in 2030.*

[124] Executive Office of the President, *Artificial Intelligence, Automation, and the Economy.*

[125] Ibid.

[126] **Metz, "The AI Threat Isn't Skynet."**

[127] Executive Office of the President, *Artificial Intelligence, Automation, and the Economy.*

Time: Exploring the 4th Dimension of Strategy

Joseph Andrew Brooks

*Time is tacitly understood and often taken for granted; it is a complex multi-faceted construct that must be fully understood for cogent strategy formulation. Through a multidisciplinary survey of the fields of history, anthropology, science, sociology, and psychology, this paper provides strategic leaders with a deeper under**standing of time's many facets. Moreover, this paper enriches the** strategic planning process by exposing the assumption of absolute time. Time is not absolute; it is relative to the observer scientifically and culturally. Strategic leaders who grasp the frontier of relative time can make use of national instruments of power to strategically manipulate time to achieve desired ends.*

Keywords: *Conflict Duration, Ethnography, Cross-Cultural Savvy, Relativity, Einstein*

Time plays a central role in the life of a nation, its culture, its security, and its international relations. Time is always a factor in operational planning, but it is often taken for granted strategically. Sun Tzu, Mahan, Clausewitz, and other theorists note that the course of a conflict is driven by the characteristics of the people involved, including cultural aspects.[1] Time is relative, not only scientifically, but in how it is perceived among individuals and cultures. For strategic leaders, understanding time is a critical competency.

Humans have a compound understanding of time as both a scientific metric and an intrinsically subjective construct. We can measure and track time with increasing precision, yet the more we understand it, the less absolute time becomes. While almost anyone can measure time, fundamental perceptions of time differ. These temporal asymmetries are often prominent in protracted conflicts. As the Taliban claimed: "The Americans have a clock, but we have the time."[2]

---

[1] Peter Paret, "Clausewitz," in *Makers of Modern Strategy* (Princeton, NJ: Princeton University Press, 1984), 199.

[2] Franklin Spinney, "Americans Have the Clock, But the Taliban Have the Time," *Counter Punch*, August 9, 2011, http://www.counterpunch.org/2011/08/09/americans-have-the-clock-but-the-taliban-have-the-time/.

Temporal asymmetry is more than just a different state of mind, it has practical manifestations, including affairs of the state. States measure and track time differently. Saudi Arabia, for example, only recently replaced the Islamic calendar with the Gregorian calendar used by America and the West. Even more striking: Saudi Arabia was not the last holdout from the Gregorian calendar; in Iran the year is 1395, in Israel, 5776, and in Thailand, 2559.[3] The construct of time, as well as how it is observed and applied, affects humanity in profound ways that cannot be seen simply by noting differences in calendars: Time and its perception has a profound impact on the course of human life. As Edward T. Hall concluded, **"Time is not just an immutable constant, as Newton supposed, but a** cluster of concepts, events, **and rhythms."**[4] Time and our perception of it is fundamentally tethered to our sociology, culture, and environment. It impacts our understandings of science and our relationship with technology. Time, therefore, plays a critical and necessary role in understanding conflict and formulating strategy.

Strategic leaders must abandon the assumption that time is perceived uniformly across populations. Understanding how a group, friend or foe, accounts for and experiences time can provide important and deep strategic insights. **Edgar H. Schein concludes: "The perception and** experience of time are among the most central aspects of how any group functions. When people differ in their experience of time, tremendous communication and relationship problems typically **emerge."**[5] Despite its criticality in human affairs, concisely defining time is a challenge.

What is Time?

Telling the time is easy; defining time is much harder. Most simple dictionaries hold time to be a measurement of past, present, **and future. Definitions of this type do not clarify the word's deeper** meaning. Science allows us to understand that time is not a natural given; time, rather, is a human creation—a social construct derived from history, religion, science, and technology—that exists relative to the observer.[6]

Time: A Brief History of the Construct

The idea of time evolved differently across the globe, but enjoys a common developmental path. Time as a construct links human existence to the natural world, celestial bodies, and spiritual realm. Babylonian, Egyptian, and Greek efforts to understand time and track its passage formed a backbone for Renaissance Europe and the development of the modern Western construct.

As early as 3,000 BCE, the Sumerians and Babylonians used their sexagesimal (1/60ths) system to chart the movement of the sun and stars. The sky was divided into degrees, minutes, and seconds.[7]

---

[3] **"The Prince's Time Machine: Saudi Arabia Adopts the Gregorian Calendar,"** *The Economist Online*, December 17, 2016, http://www.economist.com/news/middle-east-and-africa/21711938-hauling-saudi-arabia-21st-century-saudi-arabia-adopts-gregorian.

[4] Edward T. Hall, *The Dance of Life: The Other Dimension of Time* (Garden City, NY: Anchor Press/Doubleday, 1983), 13.

[5] Edgar H. Schein, *Organizational Culture and Leadership*, 4th ed. (San Francisco: Jossey-Bass, 2010), 125.

[6] **Heejin Lee and Jonathan Liebenau, "Time and the Internet at the Turn of the Millennium,"** *Time and Society* 9, no.1 (March 1, 2000): 44, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.24.2749&rep=rep1&type=pdf. Note: A social construct for the purpose of this paper is "a social mechanism, phenomenon, or category created and developed by society; a perception of an individual, group, or idea that is 'constructed' through cultural or social practice." Dictionary.com, "Social Construct," 2014, http://www.dictionary.com/browse/social-construct.

[7] BCE and CE are used interchangeably with BC and AD. BCE and CE are embraced by historical communities as they do not have as strong Judeo-Christian overtones.

While precise horology—the study and measurement of time (using minutes and seconds)—remained beyond reach, Babylonian efforts culminated in the development of a 12-month calendar.[8]

To Egyptians, time was very much a God-given cycle, serving primarily to understand and predict natural events such as the flow of the Nile and the changing of seasons. The Egyptians are credited with the 365-day year and duodecimal (1/12ths) sundials from ancient Egypt (1500 BCE) are precursors for the 24-hour day.[9] Given solar reliance, the duration of the hour was not standardized and precision following sundown was difficult. Nocturnal Egyptians would track time with the moon, stars, water clocks and other gravity-driven time approximators.[10] More than a millennium later, the Greeks would synthesize Babylonian and Egyptian time concepts to better reconcile the interplay between their gods, their world, and the cosmos.

By 127 BCE, the Greek scholar Hipparchus standardized the duration of an hour to allow for more accurate astronomical calculations.[11] This standardization was essential to Ptolemy's trigonometric calculations that in turn aided astronomers and navigators alike.[12] Even though the Greeks standardized its measurement, time remained the property of the gods. The Greeks had two words for time: Chronos and Kairos. Chronos, named after the god who informs our modern image of Father Time, described time's sequential and unyielding flow. Kairos described the opportune or historical moment and was a fundamental concept in Greek philosophical notions of fate and destiny.[13]

Time was not just a fascination of the Western world; it was also tracked in China, albeit with less precision and persistence. The Chinese, per imperial decree, developed the first functioning mechanical clock in 1094 CE to anticipate the movements of the sun, moon, and stars. No further effort was given to the mechanical clock, however, as it was deemed overly complicated and of little apparent benefit. For the Song and subsequent dynasties, water driven clocks were adequate for astrological duties.[14] Given time's importance in tracking the heavens and setting horoscopes, the science and art of horology were controlled by the Emperor. In essence, the Chinese construct of time was more fully an instrument of power than a scientific pursuit. Central control over time in China continues to this day. Although the nation spans five geographic time zones, Chairman Mao directed it be further unified under one time zone. This control effort remains contested as the rebellious Uyghur population in Xinjiang pointedly track their own local time.[15]

---

[8] Roni Jacobsen, "60: Behind Every Second, Millenniums of History," *New York Times Online*, July 8, 2013, http://www.nytimes.com/2013/07/09/science/60-behind-every-second-millenniums-of-history.html.

[9] Nicole Smith, "Ancient Egyptians and the Concept of Time," *Article Myriad*, January 12, 2012, http://www.articlemyriad.com/ancient-egyptians-concept-time/; Michael A. Lombardi, "Why is a Minute Divided into 60 Seconds, an Hour into 60 Minutes, yet there are Only 24 Hours in a Day?" *Scientific American*, March 5, 2007, https://www.scientificamerican.com/article/experts-time-division-days-hours-minutes/?print=true.

[10] Lombardi, "Why is a Minute Divided into 60 Seconds."

[11] Ibid.

[12] U.S. Library of Congress, "Ancient Greek Astronomy and Cosmology," https://www.loc.gov/collections/finding-our-place-in-the-cosmos-with-carl-sagan/articles-and-essays/modeling-the-cosmos/ancient-greek-astronomy-and-cosmology.

[13] Helge Jordheim, "Conceptual History between Chronos and Kairos – The Case of Empire," *Redescriptions: Yearbook of Political Thought, Conceptual History and Feminist Theory* 11, no. 1 (January 1, 2007): 116-117, 126, http://www.jyu.fi/yhtfil/redescriptions/Yearbook%202007/Jordheim_2007.pdf.

[14] David S. Landes, *Revolution in Time: Clocks and the Making of the Modern World* (Cambridge, MA: Harvard University Press, 1983), 17-37.

[15] Matt Schiavenza, "China Only Has One Time Zone—and That's a Problem The Communist Party's Decision to Use Beijing Time across the Country, Done to Enhance "national unity," has backfired in Xinjiang," *The Atlantic*, November 5, 2013, https://www.theatlantic.com/china/archive/2013/11/china-only-has-one-time-zone-and-thats-a-problem/281136/; Josh Summers, "A Tale of Two Time Zones," *Far West China*, February 2015, https://www.farwestchina.com/2015/02/xinjiang-time-a-tale-of-two-time-zones.html.

While the Song Chinese shunned mechanical clocks, time telling technology would profoundly change Medieval Europe. European horology would expand upon Byzantine, Egyptian, and Greek efforts to understand and track time through accurate mechanical clocks. Beyond its technical and scientific impact, the mechanical clock exerted profound influence on the structure of European society.

The Mechanical Clock – A Technology to Structure Society

To the early Europeans, time was larger than nature; it was tied to holy design. The Church sponsored much of Medieval and early Renaissance science and technology. As such, advances in horology were in the name of and benefit for the Church. **As "idleness is the enemy of the soul," initial** developments in European horology were aimed at standardizing measurements and doling out time for work and worship.[16] **The Church's de**sire to structure society was threatened by Pagan practices that tracked time through cyclical rhythms of nature.[17] **The Church's disdain for time's cycle** is evident in **St. Augustine's** *The City of God* in which linear time is described as the holy path and that **"circuitous paths" of time are the work of "deceiving and deceived sages."**[18] Religious desires for near absolute notions of time promoted the refinement and propagation of the mechanical clocks in Europe.[19]

After 1320 CE, places of worship were equipped with mechanical clocks which alerted Europeans to the passing of time through visual and audible cues.[20] Based on Hellenistic calculations, these clocks were designed to correspond to astronomical movements.[21] Church bells usurped the natural **signs of time's passing as Europeans organized their lives around the clock's persistent and** predictable pronouncements.[22] This mass synthesis of technology and pious thought created the Western construct of time.

Time's arrow and absolute time best characterize the Western construct of time. Time's arrow maintains that time is an unrelenting, single progression that links past, present, and future in a causal string.[23] **Time's arrow conforms to deep Judeo**-Christian beliefs of progression and underpins prevalent paradigms such as Newtonian physics and Whig History.[24] Stephen Hawking reckoned

---

[16] Benedict of Nursia, "The Rule of Saint Benedict," http://www.goodreads.com/quotes/329323-idleness-is-the-enemy-of-the-soul-and-therefore-the. Note: This quote is attributed to St. Benedict of Nursia and continues "...and therefore the brethren ought to be employed in manual labor at certain times, at others, in devout reading."

[17] Steve Taylor, *Making Time: Why Time Seems to Pass at Different Speeds and How to Control It* (Cambridge, UK: Icon Books, 2007), 107-108.

[18] St. Augustine, *The City of God and Christian Doctrine*, ed. Philip Schaff (Grand Rapids, MI: Eerdmans Publishing, 1886), 541.

[19] Landes, *Revolution in Time*, 58-60. Note*:* The first historical reference to a mechanical clock dates back to 1094 in China – Su Sung created a mechanical clock at the request of the Emperor of China. Landes concludes that this invention fell out of favor as there was no cultural affinity for more precise measurement of time than was already provided to the Chinese by the water driven clocks of the era (pages 17-24 of *Revolution in Time*). Landes adds that one possible and likely motivation for precise mechanical clocks was a desire by the Holly Roman Church to synchronize worship times (pages 59-61 of *Revolution in Time*).

[20] Ibid., 53-61.

[21] Ibid.

[22] Helga Nowotny, *Time* (Cambridge, UK: Polity Press, 2005), 37.

[23] Jay Gould, ***Time's Arrow Time's Cycle: Myth and*** *Metaphor in the Discovery of Geological Time* (Cambridge, MA: Harvard University Press, 1987), 13; Hall, *The Dance of Life*, 44.

[24] Gould, ***Time's Arrow Time's Cycle***, 11; Murray N. Rothbard, "The Progressive Theory of History," September 14, 2010, https://mises.org/library/progressive-theory-history.

that absolute time "is what most people would take to be the commonsense view."[25] The European construct held time to be an immutable truth that could not be challenged.[26]

Following the larger Renaissance and Enlightenment trends, clock making, horology, and astronomy eventually became more secularized. New commercial sponsors of scientific and technological study championed the importance of the clock as it aided in navigation and trade. Navigationally, mechanical clocks had to divide the passage of time into more acute increments. The **clock's increasing accuracy would reshape** both the order of society and scientific understanding of the universe.

Precise Time

Modern scholars point to the development and proliferation of mechanical clocks as an essential development in Western society.[27] Mechanical clocks provided Europe with a decisive advantage in cartography, navigation, and exploration from the 15th to 19th centuries. More precise ship bound clocks (losing only 1/10th of a second each day), such as the one invented by Englishman John **Harrison in 1764, led to the "discovery," or rather, the more precise application of longitude.**[28] Longitude enabled more expeditions and trade missions. Clocks helped naval powers (e.g., Britain) command the seas and exert diplomatic and economic power.

The clock and the pursuit of tracking time have allowed for greater compartmentalization and economization of hours devoted to labor.[29] While Benjamin Franklin is credited with publicizing the concept of time being money, the industrial revolution anchored the conceptual linkage between the two in Western society.[30] Political philosopher Helga Nowotny directly addresses this, arguing that: **"In the machine (Industrial)** age, the notion of the linearity of time prevailed because time, following the laws of economics was equated for the first time with money and made into a scarce resource. Time = money was at work in the motion of the machines**."**[31] Clocks and the pursuit of time did not just change society through economics in the Industrial era; they also redrew boundaries.

The Industrial Revolution expanded production and shrank both time and space. Railways drastically reduced the transit time between towns and cities as compared with horse-powered contrivances. Characterized as **the "annihilation of time and space**," the effect of the railroad was dynamic and dramatic.[32] Before the railway, each city and town had a unique temporal identity; they set time to correspond with local observations. Clocks were set so that 12:00 PM marked the moment the Sun crossed the meridian at its highest elevation, i.e. noon. This municipal level arrangement with the Sun meant that towns further east would change hours earlier than those further west: Boston time would be 12:00 PM, whereas clocks in New York would simultaneously read 11:48 AM.[33] This variable time represented a challenge to both the practical aspect of coordinating transit

---

[25] Stephen Hawking, *A Brief History of Time* (New York: Bantam Books, 1998), 18. Note: Hawking later states the "relativity gets rid of absolute time."

[26] Ibid.

[27] Landes, "Clocks and the Wealth of Nations," *Daedalus* 132, no: 2 (Spring 2003): 20-23.

[28] Landes, *Revolution in Time*, 156-157.

[29] Nowotny, *Time*, 47; Daniel Lattier, "How the Clock Changed the World," *Intellectual Takeout*, March 14, 2016, http://www.intellectualtakeout.org/blog/how-clock-changed-world.

[30] Benjamin Franklin, "Advice to a Young Tradesman," July 21, 1748, https://founders.archives.gov/documents/Franklin/01-03-02-0130.

[31] Nowotny, *Time*, 72.

[32] Wolfgang Schivelbusch, *The Railway Journey* (Berkeley: The University of California Press, 1986), 33.

[33] The Transcontinental Railroad, "Time Standardization," http://railroad.lindahall.org/essays/time-standardization.html.

schedules and the tacit assumption of absolute time.[34] This uniquely local time was short-lived, as railroad companies implemented their own standard times and lobbied governments to designate time zones. By 1884, the International Conference on Time Zones divided the world into 24 zones.[35]

Albert Einstein, who changed our understanding of time, was born into a world of variable time and efforts to standardize time zones. His Theory of Relativity likely was influenced by this rail-driven environment of temporal change in which the railroad was thought to have "annihilated space and time."[36] Einstein would, however, eventually bind the two together to form a fourth dimension of physics.

Space-time is comprised of four dimensions: X (horizontal, or in the case of navigation, longitude), Y (vertical or latitude), Z (depth or elevation), and T (time).[37] Space-time, which Stephen Hawking explained as "the four-dimensional space whose points are events," is strikingly similar to earlier Greek notions of Kairos (the moment) rather than the immutable Chronos.[38] While the linking of space and time represented a cognitive leap, it was **Einstein's** theory of relativity that shattered **Aristotle and Newton's concepts of absolute time.** Time, according to Einstein's formulation, is affected by factors such as speed and gravity, allowing for a condition of relative time, one in which "each individual has his own personal measure of time that depends on where he is and how he is **moving."[39]** Increasingly precise chronometers have observed that time is slower on moving clocks than it is on stationary ones.[40] These observations disprove absolute time and confirm that time is relative to the observer.[41]

Time Perception

If physics maintains that time is relative to the observer, would not perception of its passing be just as, if not more relative? Theoretically**, the answer to this question is "yes;"** however, in practice, absolute time still reigns over our social thought processes. Our predisposition to such a concept—to the point where absolute time is a tacit assumption—blinds us to poignant ethnographic differences that separate us from our allies and adversaries. Time perception varies widely among different cultures and is critical to understanding the development and alignment of agendas, values, interests, goals, and, broadly speaking . . . strategy.

A Cultural Divide

Time is a highly influential force on society, **"a guide by which social life** is actively and intentionally shaped**, a model for action."[42]** Time perception—how a culture views time—is informed

---

[34] Dennis Overbye, "The Clocks that Shaped Einstein's Leap in Time," June 23, 2003, http://oregonstate.edu/instruct/hsts414/doel/einsteintime2.htm.

[35] Schivelbusch, *The Railway Journey*, 44.

[36] Overbye, "The Clocks that Shaped Einstein's Leap in Time"; Albert Einstein, "Relativity: The Special and General Theory," trans. Robert William Lawson, 1916, part II, section 9, https://en.wikisource.org/wiki/Relativity:_The_Special_and_General_Theory.

[37] Sten Odenwald, "Special and General Relativity Questions and Answers: What is a Space-Time Continuum?" https://einstein.stanford.edu/content/relativity/q411.html.

[38] Hawking, *A Brief History of Time*, 203.

[39] Ibid., 34.

[40] Einstein Online - Max Planck Institute for Gravitational Physics, "The Relativity of Space and Time," 2017, http://www.einstein-online.info/elementary/specialRT/relativity_space_time.

[41] Seth Kadish, "Time Travel Is Real. Here Are the People and Spacecraft Who Have Done It," *Wired*, November 20, 2014, https://www.wired.com/2014/11/time-dilation/.

[42] Frank A. Dubinsaks, *Making Time* (Philadelphia: Temple University Press, 1988), 14.

by that culture's history, religion, sociology, and relationship with science and technology. Knowingly or unknowingly, time perception guides human actions and decisions. Understanding a culture's perception of time is as important as accounting for its other cultural artifacts and, significantly, can provide profound strategic insight.

Scholars generally group time perception into three overarching categories: linear time (i.e. monochromatic time), flexible time (i.e. polychromatic time), and cyclic time.[43] While these types are generalized, they nevertheless provide a framework to compare time perspectives cross-culturally. In addition to linear, flexible, and cyclical time perspectives, social psychologist Geert Hofstede adds duration preference to the discussion of cultural differences. Multiple cross-cultural surveys overwhelmingly demonstrate the existence of cultural biases regarding the duration of an investment, conflict, or engagement both in measured and perceived time. Evidence reinforces previously held notions that some cultures have a short-term orientation (STO) while others maintain a long-term orientation (LTO). STO cultures value quick results whereas LTO cultures are more patient, preferring to conserve resources and wait for progress toward their goals.[44] Clearly a link exists between cultural perceptions of time and duration preference—these factors, and their interplay influence conflict and strategy.

In the West, particularly in countries with strong historical Anglo-Saxon ties, time is akin to money: it is spent, it is invested, and its use is tightly scheduled.[45] Linear time cultures view time as a singular progression—an immutable arrow that proceeds from the past to the present and towards the future. Linear time is the social manifestation of absolute time and time's arrow. Schedules—the tyranny of the clock—dominate planning in linear time cultures. Linear time is more tangible, measured, and thereby scheduled in increasingly smaller and more precise increments. Edward T. Hall observed that linear time is "a classification system that orders life" and adds that "monochromatic time is arbitrary and imposed . . . it is treated as though it were the only natural and logical way of organizing life."[46]

In linear cultures, tasks are scheduled in an ordered and sequential format.[47] People in linear cultures tend to focus and orient their actions on the near future and have an STO when considering investments, projects, conflict, and effort.[48] Linear time influenced strategies will likely focus on sequential ordering of ways and means to achieve near-term ends while stressing adherence to a timetable in order to achieve quick, orderly results. This desire for immediacy can be stifled by allies or adversaries steeped in flexible approaches to time and LTO.

Flexible time cultures, like those found in Latin America, the Mediterranean, Middle East, and parts of Asia, tend to view time as not just one arrow, but multiple simultaneous arrows. Rather than satisfying ordered agendas, flexible time cultures focus on developing long-term relationships and the total number of tasks to be accomplished over longer periods. Flexible time cultures are averse

---

[43] Reynolds and Valentine, *Guide to Cross-Cultural*, 26; Dubinskas, Making Time, 7; Schein, *Organizational Culture*, 127; Gould, **Time's Arrow Time's Cycle**, 10-13; Hall, *The Dance of Life*, 41-55; Note: Cyclic time will be discussed later though some disagree as to whether it is a similar category to the linear and flexible time.

[44] Geert Hofstede, Gert Jan Hofstede, and Michael Minkov, *Cultures and Organizations: Software of the Mind* (New York: McGraw Hill, 2010), 239-276.

[45] **Franklin, "Advice to a Young Tradesman"; Dubinskas,** *Making Time*, 14; Sana Reynolds and Deborah Valentine, *Guide to Cross-Cultural Communication*, 2nd ed. (Upper Saddle River, NJ: Prentice Hall, 2011), 29.

[46] Hall, *The Dance of Life*, 45. While the quote is from page 45, pages 41-46 focus on monochromatic or linear time in good detail. Hall was one of the principle sources I used to understand and write on mono and polychromatic time.

[47] Ibid., 41-46; Reynolds and Valentine, *Guide to Cross-Cultural*, 28-29; Dubinskas, *Time*, 13-15; Schein, *Organizational Culture*, 127-134.

[48] Reynolds and Valentine, *Guide to Cross-Cultural*, 29; Hofstede, Hofstede, and Minkov, *Cultures and Organizations*, 240, 250, 255.

to measuring, as well as attempts to control time; linear time encourages focus on a single task, whereas flexible time encourages multi-tasking. Flexible time cultures also usually feature a much more centralized control/authority mindset and simple, flat command relationships. [49]

The penchant to multi-task and greater tolerance for delayed gratification combined with LTO strategies enable people in flexible time cultures to focus on the present.[50] Aphorisms and **expressions on time from flexible time cultures reflect this dichotomy: the Turks say "what flares up** fast extingu**ishes soon," while the Mongolian people hold that "profit always comes with a delay."**[51] Flexible time influenced strategies will likely encourage wider participation and focus on achieving multiple results over a longer duration. Whether in cooperation or in conflict, strategic leaders adhering to linear time perspectives will often find themselves frustrated by the broad scope and the protracted nature of strategies authored by those adhering to flexible time.

Perhaps furthest from the linear nature of Western time perception, cyclic time cultures, like **those found in East Asia, tend to embrace time's cycle.** Viewing time as a repeating progression, cyclic time cultures maintain that humans do not control time; they flow with it. Time is rooted in larger concepts of nature[52] with a higher emphasis on harmony. Individual efforts must fit into the rhythm of life rather than shape it.[53] This focus on temporal balance is apparent in Buddhist principles of mindfulness. Whereas a person from a linear time culture may view a missed deadline as an opportunity lost, a person from a cyclic culture would wait for the chance to rise again.

People in cyclic time cultures generally prefer to take time in making decisions and draw on connections and symmetry with the past.[54] Countries that embrace more cyclical notions of time, such as China, Japan, and South Korea tend to have a longer, more patient view of their labors pursue an LTO approach with investments, projects, conflict, and effort.[55] Strategies informed by cyclic time, will likely make use of patience, cite historical analogies, and be more responsive and adaptive to abrupt change.[56] Beyond broad cultural categorizations, the study of psychology provides some universal insights into how individuals perceive time.

The Role of Psychology

Due to persistent and somewhat contradictory notions of mortality and afterlife, the human mind is a battleground between urgency and patience. Is time a destroyer? Is it racing for or against us? Is it an omnipresent, yet ambivalent companion? With regard to individual mindset, the answer may depend on five fundamental psychological laws of time:

1. Time speeds up as we get older;
2. Time slows down when we are exposed to new experiences and environments;
3. Time passes quickly in states of absorption;
4. Time passes slowly in states of non-absorption,

---

[49] Reynolds and Valentine, *Guide to Cross-Cultural*, 30-31; Schein, *Organizational Culture*, 127-134; Hall, The Dance of Life, 46.

[50] Reynolds and Valentine, *Guide to Cross-Cultural*, 31; Hofstede, Hofstede, and Minkov, *Cultures and Organizations*, 240, 250, 255.

[51] Reynolds and Valentine, *Guide to Cross-Cultural*, 31.

[52] Taylor, *Making Time*, 107.

[53] Gould, **Time's Arrow Time's Cycle**, 64, 196.

[54] Reynolds and Valentine, *Guide to Cross-Cultural*, 32-35.

[55] Hofstede, Hofstede, and Minkov, *Cultures and Organizations*, 240, 250, 255.

[56] Reynolds and Valentine, *Guide to Cross-Cultural*, 32-35.

> 5. Time often passes slowly . . . [when] **the 'conscious mind' or normal ego is in** abeyance.[57]

While these laws are general and the understanding of the human psyche is a constantly evolving study, they reflect a certain intuitive appeal. Moreover, social and technological trends may heighten psychological factors of time perception.

The Role of Technology

Humanity's relationship with time changed in 2007 with the invention of the smartphone. Borrowing from a phrase first coined in climate science, academics in economics and public policy have described the post-2007 **world as "**The Great Acceleration.**"** This Great Acceleration, in social science, describes a situation where the speed of information, due to ubiquitous technology, has drastically increased the rate of change.[58] Given this acceleration, individuals expect instant gratification.[59] In this new environment, policy makers are compelled to speed up decision-making to keep pace.[60] This perceived need for greater urgency in decision-making amplifies already potent **cultural dispositions towards STO. Once the standard in business and governance, today's attempts** to conduct five-year plans, for example, seem anachronistically measured and immobile as strategic leaders are pressed to respond quickly to new information.[61]

The Great Acceleration also extends to conflict. The weapons of the cyber domain travel to their target at near instantaneous speed and information warfare is equally rapid and more powerful than ever.[62] **Taylor's second, third, and fifth laws of psychological time are clearly** at play as countries engage in cyber and information warfare. Cyber and information warfare actions are, in part, efforts to manipulate the decision environment at a psychological level. Finding their decision space beset with fast, changing information, decision-makers fear being left behind—they perceive that their time to decide and to act is running out. The Chairman of the Joint Chiefs of Staff, General Joseph Dunford recently testified to this effect: **"the** pace of change has accelerated . . . Decision space has collapsed, **and so our processes must keep pace with the speed of war."**[63] This increased need for quick decision-making may be the result of a contrived perception—the designed purpose of enemy action—and as such can be counterproductive. The strategic leader in crisis needs to detect this ruse and ensure or restore an atmosphere for thoughtful deliberation.

---

[57] Taylor, *Making Time*, quoted from 229; discussion on 5-106.

[58] Thomas L. Friedman, *Thank You for Being Late: An Optimists Guide to Thriving in the Age of Accelerations* (New York: Farrar, Straus and Giroux, 2016), Kindle e-book loc 404-**436; "The Creed of Speed: Is the Pace of Business Really Getting Quicker,"** *The Economist*, December 5, 2015, http://www.economist.com/news/briefing/21679448-pace-business-really-getting-quicker-creed-speed**; Murray Newlands, "The One Certainty About the Future** Is the Pace of Change Will Only **Quicken,"** *Entrepreneur*, January 9, 2015, https://www.entrepreneur.com/article/241255.

[59] Linton Weeks, "Impatient Nation: I Can't Wait for You to Read this," *NPR*, December 6, 2010, http://www.npr.org/2010/12/06/131565694/impatient-nation-i-can-t-wait-for-you-to-read-this.

[60] Christopher Muther, "Instant Gratification is Making us Perpetually Impatient**,"** *Boston Globe*, February 2, 2013, https://www.bostonglobe.com/lifestyle/style/2013/02/01/the-growing-culture-impatience-where-instant-gratification-makes-crave-more-instant-gratification/q8tWDNGeJB2mm45fQxtTQP/story.html**; Barack Obama, "Final Address to the Un**ited Nations,**"** *Time Online*, September 19, 2016, 17, http://time.com/4501910/president-obama-united-nations-speech-transcript/; Stewart Brand, *The Clock of Long Now: Time and Responsibility* (London, UK: Phoenix, 2000), Kindle e-book loc 431-443.

[61] Brand, *The Clock of Long Now*, Kindle e-book loc 110.

[62] Roman Dobrokhotov, "Russia's Soft Warfare: Hackers, Fake News, Freaks, Trolls, and Pranksters are Russia's New Soft Pow**er Weapon Arsenal,"** *Al-Jazeera*, February 27, 2017, http://www.aljazeera.com/indepth/opinion/2017/02/russia-soft-warfare-cyberwar-hackers-fake-news-170227070148722.html.

[63] Jim Garamone, "Dunford: Speed of Military Decision-Making Must Exceed Speed of War," *Small Wars Journal*, January 31, 2017, http://smallwarsjournal.com/blog/dunford-speed-of-military-decision-making-must-exceed-speed-of-war.

Time in Strategy

The construct of time clearly impacts strategy formation at every level. Armed with an understanding of time as a construct—including its history and its role in science, technology, culture and society—time savvy strategic leaders account for potentially varying time perception and preference among themselves and their allies and adversaries. Accounting for time perception and duration preference, however, is not sufficient to make Father Time (*Chrono*s) an ally. Strategic leaders must also capitalize on momentum, or lack thereof, (*Kairos*) and manipulate time perception through the instruments of national power and psychology to best suit desired ends, ways, and means.

Knowing Yourself

Sun Tzu emphasized the value and importance of knowing yourself and knowing your foe.[64] Knowing yourself—understanding your people and their culture—is of particular significance in a democratic system where human perception is paramount. Absolute and linear time is a tacit assumption at the center of American strategy. Decision-makers in America see time as a valuable and highly perishable resource, especially in politics **where there is a "fierce urgency of now" and** concerns about election timetables.[65] Accordingly, policy makers seek to manage and protect their time. Americans prefer quick outcomes and have a very strong predilection for STO, especially when considering the accelerant effect of modern IT.

When Americans desire a change, they want it instantaneously. Patience is almost a quaint anachronism, and protracted negotiations and conflicts are often regarded as unsuccessful blunders.[66] The desire for decisiveness has led to the adulation of leaders who take action and do so quickly. This decisiveness, however, can be a limitation, as it can artificially accelerate a conflict by forcing early action before the opportune moment—*Kairos*—has arrived. One of the most vexing challenges for the American strategic leader is striking a balance between deliberation and action. To find the time for critical thought, the American strategic leader should take advantage of the design of the government and its intrinsic system of checks and balances to regulate the pace for reaching decisions, taking actions, and managing, if not controlling, the pace of conflict. Undue haste can prevent the American strategic leader from understanding both allies and adversaries.

Knowing Your Enemy

While America subscribes to absolute, linear time, and exudes a strong preference for STO, **adversaries may not. Different time perceptions and duration preferences influence the opposition's** strategy. Strategic leaders must have a refined understanding of how their opponents view time. Previous studies are helpful, but outline matters in broad (East and West) and even sub-continental terms (East Asia, Latin America, Western Europe, etc.). To more fully understand a given opponent, ally, or situation, however, more specificity is needed. The following questions help frame consideration of the temporal aspects of the environment, adversary, and conflict at hand:

1.   How old is the conflict and is it existential to any party involved?

---

[64] Sun Tzu, *The Art of War*, trans. Samuel Griffith (New York: Oxford University Press, 1963), 84.

[65] Martin Luther King Jr, "I Have a Dream," August 28, 1963, http://www.americanrhetoric.com/speeches/mlkihaveadream.htm.

[66] Shawn Snow, "Long Wars and Ugly Nationalism Test Americans' Patience," *The Hill*, July 19, 2016, http://thehill.com/blogs/pundits-blog/foreign-policy/288188-long-wars-and-ugly-nationalism-test-americans-patience; Ronald Alsop, "Instant Gratification and its Dark Side," *Bucknell Magazine*, July 17, 2014, http://www.bucknell.edu/communications/bucknell-magazine/instant-gratification-and-its-dark-side.html.

2. How old is **the adversary's culture, nation, and state?**
3. Is there a religious aspect to the conflict?
4. How does the adversary perceive time?
5. **What is the adversary's duration preference**—STO or LTO?
6. What is the role of technology in the conflict?

A better understanding of time perception and duration preference allow strategic leaders to determine if they will face an opponent who will try to accelerate or decelerate the conflict to better suit their strategic needs and capabilities.

Understanding the history of the conflict and the adversary is essential to strategic formulations. A historical perspective is helpful in estimating the opponent**'s ability to endure conflict as well as** understanding their cultural and psychological mindset. A newcomer to an old conflict may have **milestones that are not synchronized with his or her allies' and may be potentially spoiled by a** persistent and patient foe with the experience and expectation for a long, and possibly brutal conflict. Older nations, states, and cultures can have an extended multi-generational outlook on a given conflict and a greater willingness to endure protracted wars. Finally, if the conflict is viewed as existential to any party, America may have to decide whether to confront or avoid a resilient, enduring pattern of resistance.

Just as religion played a decisive role in establishing Western constructs of time, religion may also play an important role in how the adversary and adherents view time. Religious fervor can increas**e an enemy's resolve and prolong a conflict, especially** so if that religion grants them an eternal and bountiful afterlife. Time perception and duration preferences can also create a mismatch in objectives and strategy. Flexible time cultures may approach the conflict in a less structured, but more multi-**faceted manner than America's linear default. Furthermore, cyclic cultures may be more** reactionary than cultures that follow linear or flexible time.

Finally, technology plays both a critical role in the way humans perceive time and a determinant role in conflict duration. Conflict between nuclear powers, for example, has the potential of decisive brevity whereas a guerilla war can last decades without resolution. Technological advancements enable increased conflict speed so long as the opponent is not able to disrupt or deny use of advanced **technology as a means of gaining advantage and thereby adjust a conflict's duration**.

Manipulating Time and Its Perception through Instruments of National Power

The strategic manipulation of time—the ability to increase allied decision space (decelerate the clock) or collapse adversary decision space (accelerate the clock)—is an essential consideration. Humans pace interactions through balancing expectations and practical factors. Expectations are set by psychology, cultural norms, precedence, as well as notions of risk and opportunity cost. Common practical factors include environmental conditions, path dependent schedules, and endurance limitations.[67] Anthropologist Pierre Bourdieu observes that while humans exert control over the nature, intent, and intensity of their interactions, the duration or interval of the interaction is often overlooked. This oversight is a critical shortcoming, for, **as Bourdieu contends: "to abolish the interval is to abolish strategy."**[68]

The deliberate timing of action can increase, alter, or reduce the perceived nature, intent, and intensity of an interaction. While Bourdieu points to the role of time in common human interactions

---

[67] Pierre Bourdieu, *Outline of a Theory of Practice*, trans. Richard Nice (Cambridge, UK: Cambridge University Press, 2016), 6-9.

[68] Ibid., 6.

(the offering of a gift or escalation of a feud), the practice of using time to secure victory in sports is perhaps a helpful analogy to consider matters of national security strategy.[69] The coach of a football team seeks to control the clock on game day. The coach understands his own team's preference but also remains flexible to adjust strategy if needed. The quick scoring, pass-oriented teams are usually STO in that they aim to establish dominance early and drain their opponents' resolve to outlast. Contrast this approach with the LTO of teams that feature the running game. Running teams aim to tire down their opponent physically. Despite initial preferences, each coach must have strategies to offset the other team's advantages. The coach must also adapt his strategy to game day conditions. They must decelerate the clock if they are behind or accelerate it if they are in the lead. In the context of national security, this manipulation or clock control can be accomplished through various instruments of national power.

In conflict, the idea of manipulating the strategic clock dates back to the Quintus Fabius' tactics against Hannibal in the Second Punic War. Fabius knew he could not beat Hannibal in a decisive contest, so he prolonged the conflict to exhaust Hannibal of the resources and will needed to wage war.[70] Just as in ancient Rome, culture, psychology, and environment play an essential role in how an individual leader and his or her people experience time. The strategic leader may be able to use instruments of power to change their adversary's time perception and preference (LTO or STO).

Strategic leaders can develop strategy and design approaches that use diplomatic outreach, economic and financial measures, information operations, and military deterrence to give pause to aggressors while reassuring the public that sufficient time exists for reviewing options. Conversely, diplomatic rebuffs, acute sanctions, information access disruptions, and decisive military action can reduce the adversaries' time to react (decision space). The following 20th-century examples, one from each instrument of power (DIME), illustrate the strategic manipulation of time:

- Diplomacy (D): In 1972, United States' President Nixon decelerates the clock vis-à-vis the Soviet Union with his visit to China. This action also produces an immediate improvement in relations with both China and the Soviet Union.[71]
- Information (I): In 1917, British Intelligence accelerate the clock on their adversary—Germany—when they share the Zimmermann Telegram with President Wilson. The telegram convinces America to declare war on Germany.[72]
- Military (M): In 1967, Israel, believing that they would not survive an attack from Arab nations, accelerates the clock with decisive pre-emptive strikes.[73]
- Economic (E): In 1941, The United States accelerated the clock with an oil embargo against Japan. Japan relied on U.S. imports of oil and only had a limited reserve supply. Projected shortfalls in oil accelerated Japan's timetables for war with the United States.[74]

The embargo against Japan shows how an action may inadvertently accelerate the clock. The embargo was intended to slow the Japanese war machine, but actually had the opposite effect.[75] In

---

[69] Ibid.

[70] Polybius, "The Rise of the Roman Empire," translated by Ian Scott-Kilvert, Introduction by F.W. Walbank (Harmondsworth, NY: Penguin Press, 1979), 256.

[71] UVA Miller Center, "Richard Nixon: Foreign Affairs," https://millercenter.org/president/nixon/foreign-affairs.

[72] US National Archives, "The Zimmermann Telegram," August 15, 2016, https://www.archives.gov/education/lessons/zimmermann.

[73] Sara Sudetic, "Pre-Emption and Israeli Decision-Making in 1967 and 1973," March 16, 2014, http://www.e-ir.info/2014/03/16/pre-emption-and-israeli-decision-making-in-1967-and-1973/.

[74] David L. Roll, "Oil Led to Pearl Harbor," *Salon*, December 5, 2013, http://www.salon.com/2013/12/05/oil_led_to_pearl_harbor/.

[75] The State Department – Office of the Historian, "Japan, China, the United States and the Road to Pearl Harbor, 1937–41," https://history.state.gov/milestones/1937-1945/pearl-harbor.

short, the several examples demonstrate how timing the use of instruments of power impacted the strategic clock.

Conclusion

Understanding the clock—ours, our allies, and our enemies—is an important extension of understanding the environment. Though commonly associated with limitations, deadlines, and restrictions, time is relative and relational. By accounting for different cultural time perceptions, strategists engage another dimension of empathy and cross-cultural savviness, potentially enhancing the ability to: escalate or de-escalate a conflict, accelerate or slow the tempo of operations, influence **others' perceptions of time**, and frame decision-making with greater options for what, when, and how long. The United States, with its extensive and capable instruments of national power, has the capability to control the clock in nearly every conflict. Time and time perception are mutable . . . with that knowledge, strategic leaders can purposefully leverage the fourth dimension to meet desired ends.
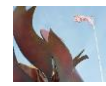
Deception: A Supplement to Instruments of National Security

Patrick B. Quinn

The shift from a relatively stable bi-polar world has increased the need to supplement existing instruments of national power. To supplement national power without increasing costs, the U.S. should study and apply strategic deception. Deception is an effort to manipulate and distract an opponent in order to shift the strategic picture, creating operating space for both political and military actors. The returns for a modest investment in deception greatly exceeds the initial costs. Examined here are Iraqi strategic deception efforts against Iran and against the Gulf War coalition, and the 1973 Egyptian deception campaign against the Israelis. Deception operations should be codified into policy at the national level, where they can then be integrated down the chain of command into the agencies and the military. The Defense Intelligence Agency would coordinate, train, and monitor the effectiveness of Deception Planning Cells staffed by field grade officers with the Additional Skill Identifier (ASI) of Deception Planner. The military could initiate a cultural shift embracing the use of deception in planning and operational cycles, thus paving the way to incorporate deception into the other national instruments of power.

Keywords: *Yom Kippur, DIA*

We are never deceived; we deceive ourselves.

—Goethe[1]

In only one generation, the modern world radically shifted. Following the Cold War, the collapse of the USSR, and the end of a unipolar world, competing regional powers and non-state actors have changed the strategic environment; globalization and technology have blurred the lines between tactical and strategic; the traditional Westphalian system of state actors is challenged by transnational groups and the number of states in crisis or failure; and climate change and the spread of nuclear weapons have accelerated. In this highly complex environment, the U.S., along with its

[1] Goodreads, "Jonathan Wolfgang von Goethe: Quotes: Quotable Quote," http://www.goodreads.com/quotes/93663-we-are-never-deceived-we-deceive-ourselves.

allies, will have to spend more to maintain their national interests in rules-based global security and prosperity. The judicious use and application of strategic deception is one means of maintaining international security in a more complex world without increasing associated costs, especially with finite resources and the American electorate increasingly reluctant to shoulder the costs associated with maintaining *Pax Americana*.

A low cost, but highly effective mechanism, strategic deception:

- generates strategic breathing space by creating imbalances in opponents.
- is a highly complex effort, requiring knowledge of the opponent, and reliance on close coordination of multiple stakeholders.
- is an art that must be designed and practiced by a professionalized cadre within the military charged with coordinating operations as a part of a whole-of-government strategic plan.
- is an effort to take active steps to manipulate and distract an opponent while creating an opportunity to take unanticipated decisive action.
- pushes **the opponent's decision makers towards a plausible but incorrect conc**lusion, carefully aligned with **that opponent's cultural and historical biases.**
- plays on many levels to create a background which supports the proffered conclusion.
- creates a strategic space for the deceiver, and positions the deceived at a disadvantage.
- is inexpensive relative to outcome.

Because strategic deception offers a means of unbalancing or even manipulating an opponent, it presents an opportunity to attain a more beneficial strategic position without having to commit all available resources.

Studies of Practical Strategic, Operational, and Tactical Deceptions

History provides some excellent examples of deception operations, both successful and unsuccessful. Examined here are Iraqi strategic deception efforts against Iran and against the Gulf War coalition, and the 1973 Egyptian deception campaign against the Israelis. Examples of successful deceptions confirm the tenet that deception manipulates an opponent into undertaking an action and requires both an understanding of the target and coordinated messaging across the scope of a campaign. The deception efforts examined here were inexpensive relative to their successful outcomes.

Iraqi Deception Efforts in 2003 and 1991

With strategic messaging about Weapons of Mass Destruction (WMD) in 1999-2003, Saddam **Hussein and the Iraqi high command present an interesting twist on Hitler's or Churchill's public** pronouncements during World War II.[2] Saddam had two separate and nearly contradictory messages to send, one to the international community and one to his enemy Iran about his WMD programs. **Saddam was in a bind, "... simultaneously attempting to deceive one audience that they were gone,**

---

[2] Barton Whaley, *Stratagem: Deception and Surprise in War* (Cambridge, MA: Center for International Studies, Massachusetts Institute of Technology, 1969), 161. **Churchill's constant and public talk in 1943 about the "soft underbelly of Europe" caused the German high command to believe an Adriatic invasion was possible even with scant evidence. They** continued to garrison Wehrmacht formations in Yugoslavia rather than move them to oppose actual Allied landings in northern Europe. Hitler too used a similar tactic in 1941. He publicly and repeatedly said he would not enter in to a two-front war, yet launched Operation Barbarossa while fighting in W**estern Europe. Any discovered evidence of Barbarossa's** troop buildup in the East was explained away as preparations to invade England.

and another that Iraq still had them."[3] Iraq had used chemical and biological weapons to halt Iranian human wave attacks in the Iran-Iraq War. Saddam had also used them against his rebellious Kurdish subjects. Post-Gulf War documents led to the discovery of a secret Iraqi quest to build nuclear weapons. By 1998, Iraq was under a UN mandate to destroy all its WMD stockpiles, and had demonstrated its willingness to appear to mislead UN weapons inspectors operating under the United Nations Special Commission (UNSCOM).[4] Examples included when weapons inspectors were denied entry to military facilities at the same time as the Iraqi military was seen to be moving equipment out of the facilities. Iraqi military units discussed removing the terms "nerve gas" from their radio traffic.[5] Despite this apparent evidence, the UN weapon inspectors never found proof of Iraqi WMD. The entire effort seemed to show that Iraq was hiding WMD from inspectors.[6] Saddam made the calculation that it was better to have the UN suspect he was cheating by keeping WMD, than to make himself vulnerable to the Iranians or his own restive population by admitting he had come clean on his weapons program. Even as U.S. military forces were gathering in Kuwait, Saddam still did not believe the U.S. would drive to unseat him, while he knew very well that an internal coup or a successful Iranian invasion would result in his death.[7] His deception plan against the UN targeted the weapons inspectors themselves, with the idea they would report his crafted narrative to the UN main body. His deception plan against Iran included strategic messaging of his military capabilities through the expectation that the UN would publically accuse him of having chemical weapons. His pronouncements, and not so hidden subterfuge, were a clever use of strategic messaging to upset Iran's military calculus, and bolster Iraq's internal and external defense.

Following the invasion of Kuwait in 1990, the Iraqis ran a media campaign broadly aimed at their Arab military opponents. It was designed to show the American forces as weak, cowardly, and unwilling to fight the Iraqis. Ironically it claimed that the U.S. forces were shifting from the fortified coastal area of Kuwait further to the west, leaving the Arab armies to fight Iraq alone. The Iraqi military based this deception effort on their belief that the U.S. forces would attack straight north from the Saudi-Kuwait border. This deception may have reinforced Iraqi analysis of coalition movements, as U.S. forces were moving to the west, and any inputs received by the Iraqis could be assumed to have come from their own propaganda.[8] In this case, internal secrecy and compartmentalization, important features of any deception plan, might have only added to the confusion. For the Iraqis, the campaign had no positive effect. While it properly targeted their Arab opponents, it violated the aforementioned concepts of using deception to force an opponent to undertake an action. This Iraqi effort was not part of a greater strategic plan; it did not serve to mask Iraqi actions, or get coalition forces to move anywhere. The poorly conceived plan backfired as it only served to potentially blind their own analysis.

[3] Kevin M. Woods et al., *Iraqi Perspectives Project. A View of Operation Iraqi Freedom from Saddam's Senior Leadership* (Norfolk, VA: U.S. Joint Forces Command, 2006), 91.

[4] Jeffery Richelson, *Iraq and Weapons of Mass Destruction* (Washington, DC: National Security Archives, February 20, 2004), http://nsarchive.gwu.edu/NSAEBB/NSAEBB80/#2.

[5] Woods et al., *Iraqi Perspectives Project*, 93.

[6] *A Decade of Deception and Defiance, Saddam Hussein's Defiance of the United Nations,* Background paper for George W. Bush speech to UN General Assembly (Washington, DC: National Security Archives, September 12, 2002), http://nsarchive.gwu.edu/NSAEBB/NSAEBB80/wmd13.pdf.

[7] Woods et al., *Iraqi Perspectives Project. A View of Operation Iraqi Freedom from Saddam's Senior Leadership*, 15, 25, 45.

[8] Kevin M. Woods, *The Mother of All Battles: Saddam Hussein's Strategic Plan for the Persian Gulf War* (Newport, RI: Naval Institute Press, 2008), 200-201.

Egyptian Deception in the 1973 Yom Kippur War

Egyptian efforts in the Yom Kippur War of October 1973 demonstrate successful strategic, operational, and tactical deceptions, against targets within Israeli leadership, military and the state. In late spring 1972, a state of 'no peace, no war' defined the Arab-Israeli status quo.[9] The stinging Arab defeat in 1967 and loss of territory did not sit well with the Arab leadership or the Arab populous, and to compound matters, Egypt's economic situation was worsening. By late 1972, Egyptian President Anwar Sadat decided that only war would break the stalemate, and with his Syrian allies began planning to launch what became the 1973 Yom Kippur/Ramadan War.

The first steps in Egypt's deception plan targeted the Israeli leadership and state, through Egyptian strategic messaging. The Egyptians and Syrians used state controlled media to broadcast an appearance of passivity. The Egyptian leadership fed the state press with reports of planned trips by President Sadat during October, the regime's attempts to rekindle diplomatic efforts at the UN, and public complaints about the low state of Egyptian Army readiness.[10] Sadat's government inquired of U.S. Secretary of State Kissinger about the potential to further discuss the UN Resolution 242. This successful Egyptian disinformation campaign can be referred to as the sounds of silence, where a quiet international environment acts as background noise which, by conditioning observers to a peaceful routine, actually covers preparations for war.[11] Unlike the Iraqi media announcements, Egyptian media efforts masked their own military preparations, and reassured the Israeli leadership and population that Egypt was not going to war.

At the operational level, which targeted the Israeli military leadership, the Egyptian deception had three main goals: inhibit consolidation of military installations on occupied land, keep Israel off balance by forcing military call ups, and lull the Israelis into a false sense of security.[12] In addition to random cross-Suez Canal shelling, the Egyptians maintained a constant state of military readiness that ensured the Israelis would have to undergo repeated call ups and mobilizations for little reason but to inure the Israelis to the multiple false alarms. Due to Israel's small population, reserve mobilizations were expensive. Prior to initiating the October attack, the Egyptians had mobilized in May, August, and September, 1973.[13] The Israelis matched the first two mobilizations with their own, but decided not to mobilize a third time. The Egyptians added to this deception by publically demobilizing troops in early October, lulling the Israelis into a false sense of calm.[14] In addition to the mobilizations and stand downs, the Egyptians conducted slipshod tactical level defensive military exercises within view of the Israeli positions while conducting offensive operational exercises deep in the desert.[15] The near comical exercises in view of the Israelis reinforced previously held Israeli perceptions of the poor readiness of the Egyptian military. The Israeli military was carefully shown what they already believed: mobilizations that had no purpose, public demobilizations, and poorly disciplined troops were manning the Suez Canal.

[9] Trevor Nevitt Dupuy, *Elusive Victory, The Arab-Israeli Wars 1947-1974* (New York: Harper and Row, 1978). Egyptian journalist Mohammed Heikal described a state of 'no peace, no war' to define the Arab-Israeli status quo, especially during the time of U.S.-USSR détente.

[10] Ossama El-Sawah, *Deception in the Ramadan War, October 1973*, Strategy Research Project (Carlisle Barracks, PA: U.S. Army War College, April 7, 1999), 18-19.

[11] Michael I Handel, *Perception, Deception, and Surprise: The Case of the Yom Kippur War* (Jerusalem: Hebrew University of Jerusalem, The Leonard Davis Institute for International Relations, The Jerusalem Papers on Peace Problems, Vol. 19, 1976), 197.

[12] Frank Aker, *October 1973 The Arab Israeli War* (Hamden, CT: Archon Books, 1985), 9.

[13] Jon Latimer, *Deception in War* (New York: The Overlook Press, 2001), 83.

[14] El-Sawah, *Deception in the Ramadan War, October 1973*, 17.

[15] Aker, *The Arab Israeli War*, 10.

Another dimension to the Egyptian strategic deception efforts exists, however: the use of a double agent. A Mossad-recruited Egyptian, Marwan Ashraf, who was Sadat's chief of staff, might have been a plant feeding false information to the Israelis.[16] This agent could, like the British Double Cross system of WWII, have reinforced Israel's assessment by providing an ostensibly third party source.[17] The asset added to his legitimacy by reporting the possibility of an invasion only a few hours before the invasion took place. The asset also revealed Sadat's war aims, which were to achieve limited territorial gains, and be in a better position to restart negotiations with Israel. The last piece might have been Sadat's messaging to his opponent that he would not be driving to Jerusalem, and thereby trigger an Israeli nuclear defense. If true, the use of a double agent demonstrates the high level of skill which Egypt used in its broad-spectrum deception planning.

The Egyptian deceptions for the October War were successful from the strategic to the tactical levels, and accurately targeted Israeli leadership, military and population. Each aspect of the deception supported the other and fit into a simple grand stratagem: lull the Israelis. The Egyptians created a mood of bellicose rhetoric, but which was not matched by any major military efforts. The plan did not try to change Israeli perceptions, but instead encouraged the misperception that the Egyptian military was unprepared, and incompetent. Israeli leadership and the state received Egyptian strategic messaging via the media, while the Israeli military was duped by staged military exercises. The successful deceptions at all levels allowed Egyptian units to cross the Suez Canal, penetrate the Bar Lev Line, and drive deep into the Sinai, successes that would not have been possible without its deception plan.

Deception's Purpose, Targets, and Requirements

If successful, the deceiver's psychological efforts create physical disadvantages of time, space, or resources. For a comparatively small investment of money and personnel, armies have achieved surprise at the tactical and strategic levels. An opponent surprised is an opponent initially unable to offer calculated effective resistance. In Operation FORTITUDE, using only a few thousand troops, and careful message coordination at the senior level, the World War II Allies deceived the Germans as to the D-Day landings.[18] While the U.S. military learned and applied great lessons from WWII, one lesson that was left to atrophy was the use of strategic deception. Unfortunately, the skills learned from this strategic, multi-service, and multi-national effort were not incorporated into post-war doctrine. Even tactical deceptions can have strategic effects. In the 1990 Gulf War, U.S. forces used a scratch unit of 460 men to tactically deceive the Iraqis, while the Iraqis diverted U.S. airstrikes towards SCUD missile mock-ups in the Western Desert.[19] Both were effective small scale operations

---

[16] Abraham Rabinovich, "Our Mysterious Man on Nile," *The Jerusalem Post*, February 17, 2011, http://www.jpost.com/Magazine/Features/Our-mysterious-man-on-the-Nile.

[17] J.C. Masterman, *The Double Cross System in the War from 1939 to 1945* (New Haven, CT: Yale University Press, 1972). The British had caught and turned or imprisoned all Nazi agents in the U.K., and used these doubled agents to feed misinformation back to the German intelligence. To increase the bona fides of one agent, they had him transmit a warning of the D-Day invasion at Normandy, but only a few hours before the actual invasion. It would be too late stop the invasion, but would bolster the agent's credentials in German eyes.

[18] Roger Hesketh, *FORTITUDE, The D-Day Deception Campaign* (Woodstock, NY: The Overlook Press, 2000). Operation FORTITUDE was the cover name given to the massive U.S./UK multi-year effort to convince the German High Command that the Allied invasion would fall at Pas De Calais and not Normandy. It involved the use of false radio signals, dummy equipment, fake armies with real commanders (General George S. Patton, Jr.), and coopted Nazi spies. As the ULTRA Program decoded encrypted German signals, the Allies could monitor the effectiveness of FORTITUDE. The German General Staff and Hitler were persuaded that Calais was the real target of the invasion, and withheld Panzer reinforcements which could have defeated the Normandy landings.

[19] U.S. Marine Corps, *Liberators of Kuwait City: 1st Marine Division, Desert Shield and Desert Storm, Aug. 8, 1990 – Feb. 28, 1991* (Camp Pendleton, CA: U.S. Marine Corps, 1992), 74-77; Charles J Quilter, *US Marines in the Persian Gulf,*

that had strategic cons**equences. Each of these three deceptions were responsible for the opponent's** strategic misapplication of massive efforts and resources.

Because d**eception is manipulating an adversary's perception to create an advantage while** disguising true objectives or capabilities, it targets decision makers and their roles within their organizations. This requires solid understanding of the opponent and the creation of narratives at multiple levels within multiple facets of power. These narratives must be tightly coordinated to be mutually supporting while closely mirroring objective truth. Deception is facilitated by innate human psychological biases. Because of the complexity of deception operations, they engender their own specific requirements. Joint Publication 3-13.4 has provided a basic list of six principle requirements needed to conduct military deception operations: focus, objective, centralized control, security, timeliness, and integration.[20] These principles define the information needed to design a deception stratagem.

Deception is a psychological tool for manipulating an opponent into undertaking physical action. Deception is not failing to provide the truth; rather it is setting up an appealing alternative. Opponents are rational actors who will examine any situation and make predictions of potential outcomes. So too must the deceiver examine and predict those objectively viable outcomes before beginning to craft a deception plan. The crafted plan uses multiple means to make one of the existing options look more attractive than the others. Deception is based on what is possible, so the option **presented by the deceiver must look eminently reasonable, logical, and fit within the opponent's** frame of expectations.[21] The deceiver wants the victim to make a specific choice and move toward the selected option.

Carefully constructed deception operations target the facets **of an opponent's decision making** apparatus by focusing on three core elements: leadership, the military, and the state (or human population). Within the structure of those targets, deception operations provide information to all targets ranging from the strategic to the tactical. Deception information is also coordinated so as to be mutually supporting across the facets of leadership, military, and state. Deception thus requires an understanding of the target, highly coordinated messaging at all levels, and integration with other instruments of strategic national power. Deception may individually target the leadership, the military, and the state, but a concerted, culturally accurate, mutually supporting effort is more effective. In a successful deception campaign, an opponent looks to obtain confirmation of a hypothesis and is deceived upon finding it supported by every input from tactical to grand strategy, and extends across to the other elements of leadership, military, and state.

1990-1991: With the I Marine Expeditionary Force in Desert Shield and Desert Storm (Washington, DC: U.S. Marine Corps, History and Museums Division, 1993), 65; Charles W. Kershaw, LtCol, U.S. Marine Corps, Commander, Task Force Troy, telephone interview by author, November 7, 2016. A 460-man multiservice scratch unit, commanded by U.S. Marine Corps LtCol Kershaw used a combination of mock ups, live fire, and close air support to mimic the presence of the 2nd Marine Division. The division had disengaged and begun its movement to new positions far to the west. Postwar interviews **of Iraqi forces confirmed the deception's success as the Iraqis continued to believe they were facing the entire 2**nd Marine Division; Kevin M. Woods, David D. Palkki, and Mark E. Stout, eds. *The Saddam Tapes: The Inner Workings of a Tyrant's Regime, 1978–2001* (Cambridge: Cambridge University Press, 2011), 187. In 1990, Iraqi SCUD Force Commander LTG Hazam Ayubi used only a few men to build a series of 26 decoy SCUD missiles and launchers that were emplaced among their real launch sites. Throughout the period of hostilities, multiple squadrons of U.S. airpower were expended against the launchers (both real and mock-ups) instead of their primary mission of striking command and control in Baghdad.

[20] U.S. Joint Chiefs of Staff, *Military Deception*, Joint Publication 3-13.4 (Washington, DC: U.S. Joint Chiefs of Staff, January 26, 2012), I-6.

[21] Hesketh, *FORTITUDE, The D-Day Deception Campaign.* In 1944, the German General Staff had enough information to know an invasion of Europe was imminent, and understood that the French coast between Cherbourg and the Pas de Calais had several viable invasion locations. Operation FORTITUDE played on both the General Staff and on Adolf Hitler to make Calais appear the more logical. Without the deception plan, the German Army would have considered either beach to be a viable invasion point from England. The deception plan merely tipped the balance towards one of two logical choices.

The opponent's leadership is the most important actor in any deception plan. Leadership makes and implements the decisions that are the physical manifestations of the deceiver's planned psychological approach. The deceiver's goal is to produce an action or an inaction in support of the deceiver's intentions. Since leaders differ in making and implementing decisions, any deception plan requires a solid understanding of the leadership's role and how it operates within its own system. A deception plan may use multiple avenues to communicate its particular message, but all parts of the message are tailored to appeal to the target. By understanding how leadership makes decisions, deceivers create the conditions that guide the deceived.

The importance of the deceiver's approach aimed at the military is second only to the tailored approach to the leadership. Military planners usually focus on the physical elements of their opponents' forces. The deception effort guides the opponents' military leadership into making a wrong choice. Deception calls for a unique creation that appeals to a defined audience. As with the leadership and the state level deceptions, military deception too is only part of a strategic whole. It will be mirrored at all levels from senior military leadership down. Deceptive efforts must be coordinated and mutually reinforcing of the overall narrative.

Since there are fewer decision makers in the leadership and the military than in the state, deception efforts aimed at the state (population at large) are lower in priority, more broad in scope, and entail exploiting the organs of the governing apparatus. A deception plan for the populace does not have to be as carefully tailored as the approach to leadership. It does require, however, a deep cultural understanding of norms and must align well with the overall strategic plan. With the state or the population as the target audience, other instruments of national power have more opportunities to support the stratagem. Here, propaganda and other information operations create an atmosphere which can elevate a deception plan to the realm of the believable. As deception's goal is to have an opponent to undertake an action, and as it is difficult to motivate an entire population, deception against a state is more effective when it is used to create an atmosphere that both supports and is consistent with other ongoing deception operations.

Fundamentally two types of deception operations exist: reinforcing an existing perception or changing a held perception. Deception's target is a human being's concept of reality, and humans are filled with psychological biases. Two of the most important for deception are (1) cognitive biases, where people attempt to align evidence with a predetermined conclusion, and (2) anchoring biases, where the first received information sets the tone for all further information received. Psychology demonstrates that humans are more likely to cling to extant or preferred perceptions, rather than to accept change.[22] "With respect to deception, one overwhelming conclusion stands out: It is far easier to lead a target astray by reinforcing the target's existing beliefs, thus causing the target to ignore the contrary evidence of one's true intent, than to persuade a target to change his or her mind."[23] Since changing perceptions is more difficult, the deceiver should focus on exploiting cognitive biases, reinforcing existing perceptions by providing what the opponent wants to see while altering the trajectory of belief (or "reality") to attain strategic advantage.

The second approach, anchoring bias, helps the deception by ensuring that future inputs are defined and limited to fit the initial narrative. All organizations, whether modern stratified armies or small terror cells, conduct a basic analysis of any situation: perceived inputs, calculation, and response. In government organs, analysts work to create clarity from the inputs they receive. When

---

[22] Jonathan Haidt, *The Righteous Mind, Why Good People Are Divided by Politics and Religion* (New York: Vintage Books, 2013).

[23] Richards J. Heuer, "Strategic Deception and Counterdeception," *International Studies Quarterly* 25, no. 2 (1981): 298.

operating under pressure to divine their opponent's intentions, analysts will often make early judgments based on less than clear inputs.[24] A deception plan needs to allow enough time for the targeted analysts to perceive and examine the false option. "**Perceptions** are quick to form but then resist change. Once we have formed an impression about an object, event, or situation, we are biased toward continuing to perceive it in the same way."[25] As analysts make judgments early in the assessment cycle, beginning the deception operations as early as possible makes sense and allows time for an opponent to accept (and hopefully defend) the false narrative even in the light of true evidence.

An example of an effective multi-layer stratagem targeting leadership and the state occurred prior to the U.S. entry into World War II. Britain was battling the Nazis alone, while the U.S. remained neutral. The British stratagem forsook the military and instead targeted American **legislators' support for isolationism, and the American popu**lation. This was a direct effort to influence U.S. lawmakers, and in turn shift U.S. policy towards support for Britain.. The U.S. national strategy of isolationism was attacked, and public opinion was swayed by media manipulation. Senior U.S. political and cultural figures who supported isolationism were besmirched. **By the war's end, the term 'isolationist' had become** something of an insult. British success came from knowing the target, coordinating the messages they introduced from the lowest to the highest levels, and eventually influencing the U.S. leadership.[26]

Challenges and Opportunities of Deception in 2020-2025

Given that strategic deception is both effective and relatively inexpensive, it has particular **relevance for the U.S. in today's resource** constrained and uncertain world. Future national security operations will require more attention to deception than is currently being applied. To reach a point where the broad application of strategic deception becomes normal requires the tools and a supporting philosophy which encourages deception. The incorporation of deception planning and operations into national strategic decision making should begin with defense policy codified at the national level and mirrored through the chain of command into the agencies and the military.

The last 15 years have witnessed a tectonic shift in the availability, dissemination and control of information, all of which affect deception operations. The ubiquity of smart phones, combined with the near universal access to the internet, have changed the whole dynamic of how people and organizations receive and process information. The time surrounding sending and receiving messages has collapsed, as strategic messages can now be instantaneous. The ease by which individuals can enter into the domain of what was previously only available to intelligence services or the publishing industry creates a paradox of more information but potentially less understanding. An intelligence analyst receives collected information, studies it, draws conclusions, and publishes intelligence reports. As the analyst receives information, she or he requires more confirmation of the

---

[24] Ephraim Kam, *Surprise Attack, The Victim's Perspective* (Cambridge, MA: Harvard University Press, 2004), 91.

[25] Heuer, "Strategic Deception and Counterdeception," 297.

[26] Thomas E. Mahl, *Desperate Deception: British Covert Operations in the United States, 1939-44* (Washington, DC: Brassey's, 1998). Mahl details a multi-year effort to use the media to sway the American electorate and in turn their representatives, combined with direct pressure on U.S. legislators. The campaign was supported by wealthy and powerful Americans who had close ties to Britain. The effort worked because the deceivers intimately understood those touchstones which defined American culture. Pro-British propaganda set the stage to shift popular U.S. perceptions. The British used the American media to hector and shame opponents, and laud supporters. They manipulated or created false polls showing broad U.S. popular support for their cause, and made sure legislators were aware of the ostensible shift away from isolationism. With this complete understanding of the target, they manipulated the American population, knowing that the population would in turn influence their leadership.

information collected. More collected information results in more confirmation requirements, which are satisfied through more collection—a vicious circle. At times, the information reaching analysts can become so great as to be overwhelming.[27] Volume affects integration of a deception plan because the deceiver wants the deceived to receive false signals from across the collection spectrum.

Modern technology has greatly increased some intelligence collection capabilities; three of the main areas are SIGINT, IMINT/GEOINT or satellite Imagery Intelligence, and the extensive growth of media platforms called Open Source Intelligence (OSINT). As each collection capability advanced, defensive measures likewise increased. Modern military radios use encoded frequency hopping communications across a wide signal spectrum, thereby practically eliminating the ability to decode the communications, or often to identify it by type. This obfuscation has the perverse effect of making it easier to replicate for deception purposes. Because clusters of overlapping cell phone signals, for example, can indicate large numbers of people in one place, that pattern of signals could be reproduced electronically to make it appear that large numbers of people are clustered together when, in fact, they are not. Satellite or Unmanned Aerial Vehicles (UAV) collected imagery has increased, but it still cannot reveal the intention behind the images. Camouflage and obscuration have mirrored observational advances. The older mass media of cable news TV, radio, or newsprint are still manipulated the traditional way: through the release of false or carefully selected information. Finally, while there is an abundance of social media reporting, valuable information becomes lost in the electronic flood.

Multi-spectrum information collection can make it more difficult to deceive given the many different ways to compare the validity of the incoming information. The advantage, however, remains with the deceiver for two reasons: (1) information flow is vastly greater, but not necessarily clearer; larger repositories of information slow analysis and once reliable sources of intelligence confirmation (e.g., SIGINT) can now be more easily and cheaply manipulated; (2) humans possess an inherent tendency to maintain previous biases and to invent excuses to ignore contrary evidence, thereby locking decision makers into a perception. Barring a shift in intelligence collection and analysis philosophy, the deceiver will still have the initial upper hand. Beyond that, only time will tell. As Joel **Brenner, former counsel at NSA, notes, "Very few things will be secret anymore, and those thin**gs **which are kept secret won't stay secret very long . . . The real goal in security now is to retard the** degradation of the half-**lives of secrets. Secrets are like isotopes."**[28] To weather inadvertent discovery or partial exposure, strategic deception must be properly designed at the outset and closely aligned with other viable alternatives.

Introducing of a major philosophical shift to consider and use strategic deception across the instruments of national security would be unrealistic and probably have little chance of success. A smaller application using a proof of concept would have a better chance of succeeding and possibly becoming a model upon which the concept could be expanded. The military y has the most experience with deception operations, and given its structure, budget, and manpower capabilities, it would be a logical branch upon which to build a proof of concept.

---

[27] Ephraim Kam, *Surprise Attack, The Victim's Perspective* (Cambridge, MA: Harvard University Press, 2004), 54.

[28] Daniel C. Dennet and Deb Roy, "Our Transparent Future. No Secret is Safe in the Digital Age. The Implications for our Institutions are downright Darwinian," April 6, 2015, https://medium.com/@dkroy/our-transparent-future-aa86a7bcfe85#.p449mig37.

Conclusion

Historically, American society has placed great value in the openness of its representative government and in the free press which holds government leaders accountable. The primary obstacle to incorporating the use of deception within the government is the deep seated American belief that deception is not fair and that it confounds U.S. values of openness and honesty.[29] Thus, while deception has its place in the arsenal of government tools, it must be carefully employed so that it **does not violate the public's trust in a free media or in the authenticity of the government itself.** Effective use of deception stratagems cannot confound U.S. values as it did during the 1990-1991 **Gulf War when the media complained that it had been used as part of the coalition's deception** campaign.[30]

Since incorporating deception as a supplement to the instruments of national power might be difficult for some Americans to accept, it would be more practical to apply it initially within a precise and defined military context.[31] Deception has the ability to help shift the strategic picture, creating operating space for political as well as military actors. Even if only used in coordination with the instrument of national military power, deception is effective in creating a strategic imbalance in opponents. The returns for a modest investment in deception greatly exceed the initial costs. In major military conflicts, Americans have at times used military deception to great effect. America, however, has never aligned its multiple instruments of national power with a grand deception plan. Although cultural and political opposition to using deception may exist, the shift of the modern world away from a relatively stable bi-polar world has increased the need to supplement traditional power while preserving resources. The military could lead a cultural shift to use deception by incorporating it into its planning and operational cycle in appropriate, effective, and responsible ways. Doing so could pave the way for incorporating deception with other elements of national power. With the changing world and opponents who exploit every opportunity for advantage, now is an opportune time to use ingenuity, intellectual power, and deception to help maintain American hegemony.

---

[29] Walter Jajko, "Deception: Appeal for Acceptance; Discourse on Doctrine; Preface to Planning," *Comparative Strategy* 21, no. 5 (2002): 352. **Reflecting a common opinion of the time, FDR's Secretary of War, Henry Stimson, said, "gentlemen do not read each other's mail."**

[30] Jon Latimer, *Deception in War* (New York: The Overlook Press, 2001), 298, Illustration #27. In 1990, the U.S. military allowed the media to report on the large number of U.S. Marines practicing shore landing and beach assaults. As intended, these reports furthered the Iraqi belief in a seaborne assault. After the war, the media accused the government of being manipulated into supporting a deception campaign. Even though the military never lied to the media, some media outlets felt angry enough to publish their displeasure.

[31] A redefinition of terms might also help overcome some pr**econceived biases against "deception," such as using the term "managing perceptions."**
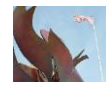
The U.S. Military. . . America's Easy Button

Scott A. Myers

*The United States continues to increase its military commitments to secure national interests at the expense of implementing other instruments of national power, despite protections deliberately **embedded into the Constitution by America's Founding Fathers to fight this outcome. The nation's** growing propensity to use military force as the primary instrument of national power is rooted in three distinct phenomena: the growing civil-**military gap, Congress's failure to exercise its** constitutional prerogatives t**o declare war, and the country's failure to ensure citizen sacrifice to** support its wars. The result is a country with an empowered Executive who frequently employs the armed forces as the primary instrument of national power to protect its interests. If not rectified, America will continue this trend **which will likely jeopardize the nation's standing and reputation.***

> [The Founders] great advice was that we should structure ourselves as a country in a way that deliberately raised the price of admission to any war. With citizen-soldiers, with the certainty of a vigorous political debate over the use of a military **subject to politicians' control, the idea was** for us to feel it – uncomfortably – every second we were at war.
>
> —Rachel Maddow[1]

Fresh from removing the shackles of British Imperial rule, America's Founders sought to install governmental and constitutional safeguards against making war. Despite these constitutional protections, the United States has increasingly turned to its military to secure or maintain national interests. In fact, over the past 40 years, the U.S. executed military operations in conflict zones over 190 times, roughly the same number of military actions that the nation conducted in the first two

---

Scott A. Myers (M.S.S. United States Army War College) is a Lieutenant Colonel in the United States Army. An earlier version of this article, written under the direction of Dr. Marybeth Ulrich, earned the prestigious Military Officers Association of America Writing Award for the USAWC class of 2017.

[1] Rachel Maddow, *Drift* (New York: Broadway Books, 2012), 202.

centuries of its history.[2] The era of U.S. hegemony following the Cold War left American power relatively unchecked while significant advances in global communications, command and control, and transportation capabilities facilitated military operations world-wide. These factors alone, however, do not explain the extent to which the United States has deviated from its foundation.

The disincentives for war that the Framers built into the American political system rely on both **citizens and Congress to fulfil their responsibilities to determine the military's role in pursuing the nation's foreign policy interest. Yet American citizens and their representatives no longer exert** meaningful in**fluence on the military's role with respect to foreign policy. Today, U.S. citizens are less** connected to the military and less affected by decisions to commit armed forces to hostilities than at **any time in America's history. To further complicate matters,** Congress has neglected its institutional responsibility for authorizing U.S. military operations. Consequently, the Executive branch gained an unprecedented autonomy to use force.

Antithetical to the Founders' vision, the widening civil-military gap, Con**gress's abdication of its** constitutional prerogatives for declaring war, and changing war-time fiscal policies have created conditions under which the U.S. too often requires the military to achieve national interests. This essay examines the origins of these conditions and proposes measures to re-engage citizens and Congress in decisions to employ the U.S. military—measures which should allow the use of all instruments of national power while decreasing its unhealthy dependence on the military.

Origins of the Citizen-Soldier Concept

Shaped in large part by their experiences with British occupation, America's Founders possessed profound beliefs on the form and function of the nation's military. Samuel Adams, for example, was among several Framers who expressed intense aversion to maintaining a standing army, arguing that **doing so would be "dangerous to the Liberties of the People."[3] Given the fledgling nation's need for a** capability to defend itself, however, an agreement was reached granting Congress the exclusive right to maintain and raise an army,[4] **but limiting Congress's ability to fund an army for a period of only two years. As such, the nation's mechanism for defending the country in times of crisis would be wartime mobilization of the states' militias** in lieu of a standing army.[5]

Despite authorizing an adequate defense capability against both internal and external threats, the Founders remained adamant that systems of governance must guard against any one individual or group waging war. As James Wilson stated to the Pennsylvania ra**tifying convention in 1787, "this** system [of government] will not hurry us into war, it is calculated against it. . . and will not be in the **power of a single man, or a single body of men." Ultimately, the Constitution became the Framers'** mechanism to protect the nation from waging war frivolously. The Founders sought to make armed **conflict difficult by granting Congress the power to declare war and by ensuring the public's sacrifice** through the use of an army comprised of citizen-soldiers. Over two and a half centuries removed from these historic decisions that shaped America, many of the safeguards the Framers instituted to prevent the nation from engaging in frequent conflicts have been circumvented, removed, or degraded to such a degree that waging war has become relatively easy.

---

[2] Barbara Salazar Torreon, *Instances of Use of the United States Armed Forces Abroad, 1978-2016* (Washington, DC: Congressional Research Service, October 7, 2016), 10-34, https://fas.org/sgp/crs/natsec/R42738.pdf.

[3] **Samuel Adams Heritage Society, "Samuel Adams Letter to James Warren, 1776,"** http://www.samuel-adams-heritage.com/documents/samuel-adams-to-james-warren-1776.html.

[4] *The Constitution of the United States,* Article I, Section VIII, Clause II, http://constitutionus.com.

[5] *Ibid.,* Clause XV.

The Widening Civil-Military Gap

In 1945, over 9 million citizens served in the U.S. military, which represented over 9-percent of the total population. At the height of the Vietnam war, the U.S. military was a 2.7-million-person conscripted force, with over 4-**percent of the nation's eligible population having served in that** conflict.[6] Today, less than one-half of one-percent of Americans serve in the armed forces. This represents an unprecedented gap between U.S. citizens and the military—one that cannot be explained simply by the inevitable and continual widening of the civil-military gap as the size of the population increases and the military end strength remains relatively stable. Aside from decreasing proportions of American veterans in the citizenry, several additional factors emerged over the past decades that expanded the civil-military divide and placed the connection between American citizens and its military in even greater jeopardy: base closures, recruitment, ROTC reductions, and multigenerational military families.

Base Closures: Over the past 25 years, the Department of Defense (DoD) closed more than 350 **military installations according to the Base Closure and Realignment Committee's (BRAC)** recommendations.[7] As a result, DoD consolidated personnel from the losing installations to several **of the military's larger** bases, creating a less geographically dispersed military force. The Army installation at Fort Bliss, Texas is emblematic of the **military's** geographic consolidation that resulted from BRAC. Its military population grew from 10,000 soldiers in 2005 to over 33,500 soldiers in 2014. Similar consolidations took place at Fort Bragg, North Carolina, Fort Hood, Texas, and Fort Carson, Colorado. The by-product of base reductions and the formation of mega-bases created a more regional military (see figure 1). In 2015, over forty-nine percent of the U.S. military served in five states: California, Virginia, Texas, North Carolina, and Georgia.[8]
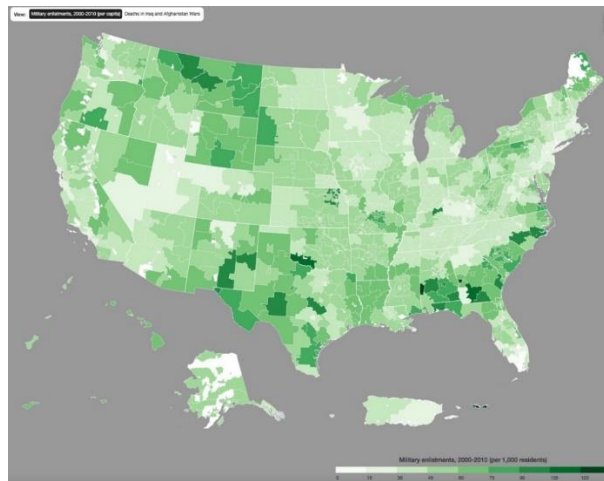

Figure 1. Per-capita Military Enlistments from 2000 to 2010[9]

---

[6] David Zucchino **and David S. Cloud, "U.S. Military and Civilians are Increasingly Divided,"** *Los Angeles Times Online,* May 24, 2015, http://www.latimes.com/nation/la-na-warrior-main-20150524-story.html.

[7] GlobalSecurity, "Base Realignment and Closure (BRAC)," http://www.globalsecurity.org/military/facility/brac.htm.

[8] Zucchino and Cloud, "U.S. Military and Civilians are Increasingly Divided."

[9] James Fallows, "The Tragedy of the American Military," *The Atlantic,* January/February 2015, http://www.theatlantic.com/magazine/archive/2015/01/the-tragedy-of-the-american-military/383516/.

Recruitment: As the nation's military progressively moved South and West, recruiting efforts and trends followed.[10] Military recruiters shifted their focus to states with larger military populations to capitalize on the existing military exposure and traditionally high recruiting rates in those states. From 1979 to 2014, military recruits from the South and West were over-represented while those from the Northeast and Midwest were under-represented.[11] The shift in military populations to the South and West further cements a regionalized military that has progressively become less connected to American society.

ROTC: Another factor contributing to the civil-military gap is the reduction and increasing **regionalization of Reserve Officer Training Corps (ROTC) programs at the nation's universities. The** National Defense Act of 1916 initiated ROTC to prepare the country for participation in World War I. Since then, ROTC has been the primary commissioning source of American officers.[12] ROTC programs have also served as a hedge against a civil-military divide, providing a vital link between the military and society through institutions of higher learning. Over the past 25 years, however, that vital link has been compromised as the number of ROTC programs decreased significantly. In the 1980s, the U.S. Army maintained 420 ROTC programs. By 2016, only 275 programs remained.[13] During recent decades, economic and societal pressures forced universities and the military to reduce ROTC representation nationwide and to focus programs in the South and West. This resulted in greater regionalization of this vital commissioning source and severed a vital link between some of **the nation's most prestigious universities and the U.S. military.**

The unpopular Vietnam War and the military's controversial but now defunct Don't Ask, Don't Tell policy served as two social catalysts for change, causing a significant backlash against universities offering ROTC programs and forcing a number to close. Most notably, the Department of Defense **closed ROTC programs at some of the nation's most prestigious universities including Harvard,** Yale, Stanford, and Columbia. These schools have only recently re-established ROTC departments to **varying degrees. The reduction of ROTC programs in institutions positioned in some of the nation's** largest cities has removed a vital link urban communities and citizens, further increasing the civil-military divide. In 2011, for example, New York, Los Angeles, Chicago, and Philadelphia had a combined population of 16 million, approximately the total combined populations of Virginia, Alabama, and Mississippi.[14] Strikingly, ROTC programs in these four cities numbered 14, while VA, AL, and MS hosted 35 programs.[15]

Multigenerational Military Families: The last factor contributing to the civil-military divide is the growing trend of multi-generational soldiers. In 2011, a Pew Research Center survey of veterans and the general public indicated that 77-percent of adults over the age of 50 had an immediate family member who served in the U.S. military compared to only 57-percent of those between the age of 30 to 49. The number decreases to 33-percent for those under the age of 30.[16] The same survey reports that close to 80-percent of veterans have a parent or sibling who served in the military, and that these

[10] **Mark Thompson, "The Other 1%,"** *Time Online,* November 21, 2011, (http://content.time.com/time/subscriber/printout/0,8816,2099152,00.html#.

[11] Office of the Under Secretary of Defense, Personnel and Readiness, *Population Representation in the Military Services: Fiscal Year 2014 Summary Report* (Washington, DC: U.S. Department of Defense, 2014), 21, http://www.people.mil/Portals/56/Documents/2014%20Summary.pdf?ver=2016-09-14-154051-563.

[12] **Cheryl Miller, "Underserved: A Case Study of ROTC in New York City," May 2011,** https://www.aei.org/wp-content/uploads/2011/10/ROTC-Final-May-2011.pdf, 8.

[13] **Zucchino and Cloud, "U.S. Military and Civilians are Increasingly Divided."**

[14] **Miller, "Underserved: A Case Study of ROTC in New York City," 10.**

[15] Ibid.

[16] **Pew Research Center, "**The Military-**Civilian Gap: Fewer Family Connections,"** http://www.pewsocialtrends.org/2011/11/23/the-military-civilian-gap-fewer-family-connections/?src=prc-number.

same veterans are "twice as likely as members of the general public to have a son or daughter who has served."[17]

In 2008, nearly 60-percent of the military's general officers had children serving in the armed forces.[18] Additionally, as of 2011, nearly 100,000 military members were married to another service member.[19] The Pew survey paints younger generations as having fewer interactions with—and less understanding of—the military while also describing an increasingly insular, multigenerational military. Together these outcomes are cause for alarm as they further separate the citizenry from the military and exacerbate the civil-military gap.

Today's smaller, more regionalized, and increasingly multi-generational military has resulted in a wider divide between U.S. service members and citizens. This separation manifests itself in American society in troubling ways. The 2011 Pew survey highlighted a number of discouraging revelations: (a) 84% of surveyed post-9/11 veterans believed that the public did not understand the problems that they or their families experience while 71% of non-military survey respondents admitted that they did not understand the problems faced by the military or their families; (b) roughly 50% of the public surveyed did not believe that the wars in Afghanistan and Iraq were worth the cost and only 25% of respondents admitted that they followed these wars closely, confessing that the conflicts in Afghanistan and Iraq had little impact on their lives; (c) 83% of surveyed adults stated that military personnel and their families have made significant sacrifices since 9/11, while only 43% believed that the American people have also made substantial sacrifices.[20]

The Pew survey describes an admittedly ill-informed American public disinterested in the U.S. military and how it is employed around the world. The same year as the Pew survey was released, Former Chairman of the Joint Chiefs of Staff Admiral Michael Mullen put the problem of the widening civil-military gap in context:

> This great republic of ours was founded on some pretty simple ideas – simple but enduring. And one of them is that the people. . . will determine the course the military steers, the skills we perfect, the wars we fight. But I fear they do not know us. I fear they do not comprehend the full weight of the burden we carry or the price we pay when we return from battle. This is important because a people uninformed about what they are asking the military to endure is a people inevitably unable to fully grasp the scope of the responsibilities our Constitution levies upon them.[21]

The public's acknowledgment and willing acceptance of the large disparity between the sacrifices made by military service-members in support of the nation's wars as compared to sacrifices made the public at large strongly diverges from the Founders' intent. They sought to ensure "a vigorous political debate" over the use of the military and wanted the citizenry to "feel [war] uncomfortably – every second" the nation is engaged in war.[22] Yet, with servicemen and women deployed to Iraq and Afghanistan for over 15 years since 9/11 and around the world for longer, the nation has never "been further from. . . the idea that America would find it impossible to go to war without disrupting domestic life."[23] As the connection between the American people and its military continues to fray,

---

[17] Ibid.

[18] Miller, "Underserved: A Case Study of ROTC in New York City," 10.

[19] Thompson, "The Other 1%."

[20] Pew Research Center, "War and Sacrifice in the Post-9/11 Era," October 5, 2011, http://www.pewsocialtrends.org/2011/10/05/war-and-sacrifice-in-the-post-911-era/.

[21] Admiral Mullen, "Address to the West Point Class of 2011," speech, West Point, NY, August 2011, http://www.rememberdaren.com/wp-content/uploads/2011/08/JCS-Speech-at-West-Point-Graduation.pdf.

[22] Maddow, *Drift*, 202.

[23] Ibid.

so too has the public's influence over the role of the military. Congress and the Executive Branch are armed with a professional All-Volunteer Force (AVF) that does not require most Americans to **sacrifice anything to support the nation's** conflicts. In short, the burden for the common defense has shifted almost entirely **to the nation's military**.[24] These conditions have enabled the Executive Branch to disproportionally rely on and wield military power to address security challenges and pursue national interests.

Authorizing the Use of Force

While the American public and its military have gradually drifted apart, the civil-military gap in Congress has also grown. **For much of America's history, military service was practically a** prerequisite for membership in Congress. Today, fewer veterans serve as representatives than at **almost any time in the nation's history**. The 95th Congress (1977-1978) proved to be the high-water mark for veteran representation with 77-percent of the Congress having served.[25] In 2016, the total number of veterans fell to less than 19% of Congress.[26] What impact does the growing civil-military gap in Congress have on its decisions to use force to pursue U.S. foreign policy?

Congress maintains the exclusive authority to declare war on behalf of the nation. This power was vested as such **to ensure George Washington's vision; that the nation's r**epresentatives would vigorously debate and formally authorize force before any military expeditions. In 1806, in *The United States v. Smith*, the Supreme Court solidified this responsibility by ruling that decisions regarding whether the nation was at peace **or at war was "the exclusive province of Congress to determine."**[27] Throughout recent history, a number of presidents have balked at the requirement to involve Congress when employing military forces overseas. As a result, Congress passed the War Powers Resolution in 1973 over the objections and veto of President Richard Nixon to strengthen its war-making authorities. This act exemplified the real struggle between the executive and legislative branches on the authority to use military force.

The War Powers **Resolution represented Congress's effort to clarify and reinforce constitutional statutes and responsibilities on the use of force, and to "ensure that the collective judgment of both** the Congress and the President [applied] to the introduction of United States Armed Forces into **hostilities."**[28] This resolution mandated reporting requirements for the executive branch to Congress. Additionally, the resolution established a 60-day limit for the deployment of military forces without congressional approval, which only Congress could extend.[29] Despite its inherent constitutional authority and the additional powers granted by the War Powers Resolution, however, Congress has repeatedly failed in its duty to deliberate and authorize U.S. military interventions abroad.[30]

---

[24] Thomas L. Friedman, "The Home Team," *New York Times Online,* February 8, 2008, http://www.nytimes.com/2004/02/08/opinion/the-home-team.html?_r=0.

[25] Andrew Rugg et al., "Vital Statistics on CongressData on the U.S. Congress – A Joint Effort from Brookings and the **American Enterprise Institute,"** *Brookings Institute,* January 9, 2017, https://www.brookings.edu/research/vital-statistics-on-congressdata-on-the-u-s-congress-a-joint-effort-from-brookings-and-the-american-enterprise-institute/.

[26] Jennifer E. Manning, *Membership of the 114th Congress: A Profile* (Washington, DC: Congressional Research Service, December 5, 2016), https://fas.org/sgp/crs/misc/R43869.pdf.

[27] United States v. Smith, July, 1806, https://law.resource.org/pub/us/case/reporter/F.Cas/0027.f.cas/0027.f.cas.1233.pdf.

[28] U.S. Code Title 50, Chapter 33, Section A, War Powers Resolution, section 1541, 310, https://www.gpo.gov/fdsys/granule/USCODE-2011-title50/USCODE-2011-title50-chap33, 310.

[29] Ibid., Section C, 318.

[30] Maddow, *Drift*, 210.

Since the advent of the All-Volunteer Force, the United States has increasingly deployed its military to conflict zones, a number of which involved combat to include operations in Grenada, Panama, Iraq, Somalia, Bosnia, and Kosovo.[31] None were approved by a declaration of war. Congress last sanctioned a formal declaration of war in June 1942 against Romania during World War II.[32] Of the numerous military operations conducted since the creation of the AVF, only three were officially sanctioned by Congress when it authorized the use of military force against Iraq in 1991 and 2002, as well as in response to the 9/11 terrorist attacks.

Despite surging military operations and the tendency of recent presidents to liberally apply **Congress's 9/11 authorization to** expand their war-making abilities far beyond the scope of the Joint Resolution, Congress has demonstrated ambivalence in fulfilling its responsibility to approve military actions. This phenomenon begs the question as to why Congress is seemingly unwilling to exert its institutional prerogative. Two explanations are plausible. The first reasonable justification **centers on the American public's relative disinterest in engaging its representatives on the issue of** using military force. Absent pressure from constituencies, U.S. representatives may choose a politically safe approach and avoid deliberating military operations so as to not be held accountable for military failures. The second, more troubling explanation involves the relationship between U.S. milita**ry interventions abroad and the American military industrial complex. America's wars and** increasingly frequent military deployments tend to support and be supported by the military industrial complex. In fact, since the height of the Vietnam war, shares of the main U.S. arms manufacturers have risen over four times the rate of the overall market.[33] The post 9/11 wars have been good business for many American corporations, providing thousands of jobs and supporting local economies. Additionally, the defense industry spends millions of dollars annually in lobbying efforts to garner congressional support for assorted military programs. These programs are, in turn, aided by the increased military operations pursued by recent presidents. The military industrial complex has also been a prime player in the campaign contribution business. In fact, in 2016, the top ten defense companies contributed over $18.5 million to congressional candidates and their respective parties.[34] Despite these two logical explanations, the decreasing veteran presence in Congress plays a larger role in rationalizing congressional inaction for approving military operations.

A 21st century Triangle Institute for Security Studies (TISS) survey examined the gap between the military and American s**ociety. This project aimed to determine whether people's familiarity with** the military influenced their views on U.S. national security and foreign policy. The examination studied survey results of four distinct populations: Elite Military, Elite Civilians who attended Professional Military Education Courses but had no actual military experience, Elite Civilians with military experience, and Elite Civilians with no military experience.[35] In comparison to military elites and civilians with military service, civilian elites with no military experience were more approving of

---

[31] Jennifer K. Elsea and Matthew C. Weed, *Declarations of War and Authorizations for the Use of Military Force: Historical Background and Legal Implications* (Washington, DC: Congressional Research Service, April 18, 2014), appendix B, https://fas.org/sgp/crs/natsec/RL31133.pdf.

[32] Ibid., 1.

[33] James Petras, "The Soaring Profits of the Military-Industrial Complex, the Soaring Costs of Military Casualties," June 24, 2014, http://www.globalresearch.ca/the-soaring-profits-of-the-military-industrial-complex-the-soaring-costs-of-military-casualties/5388393.

[34] Open Secrets.Org, "Defense: Top Contributors to Federal Candidates, Parties, and Outside Groups," https://www.opensecrets.org/industries/contrib.php?ind=D.

[35] Peter D. Feaver and Christopher Gelpi, *Choosing Your Battles: American Civil-Military Relations and the Use of Force* (Princeton, NJ: Princeton University Press, 2004), 36-37.

an interventionist approach in terms of the range of issues for which they supported using military force.[36]

Rather remarkably, the TISS study also concluded that as veteran presence in the executive and legislative branches increased, the probability that the U.S. would use military force to settle disputes decreased by 90%.[37] The study postulated that as veteran presence in the executive and legislative branches continued to decline, the United States would be increasingly likely to use military force as the principal instrument of national power to address foreign policy aims.

The TISS survey and its findings are over a decade old. While no subsequent studies exist that confirm or refute its propositions, Congress's decreasing veteran presence and America's increasingly interventionist posture are consistent with appear to lend credence to the study's findings. Whether Congress's rising tendency to support military interventions is a function of its members' fundamental beliefs on the use of military force or due to acquiescence on military matters in general, neither is positive. The result is a country whose foreign policy fails to balance the use of all instruments of national power.

The byproduct of Congress's egregious failure to execute its constitutional responsibilities has been the unprecedented strengthening of the Executive's ability to commit the nation's military at will. Congress, as Thomas Friedman describes, "either meekly bows to the wishes of the executive or provides the sort of broad authorization that amounts in effect to an abrogation of direct responsibility."[38] The result is arguably a nation where the only real struggle for waging war is between the White House and the Pentagon: where war has become an almost natural condition of the American state.[39]

Paying for War

A third phenomenon that has enabled the country to drift toward conflict is the government's recent departure from levying taxes on current generations to pay for war. America has a profound legacy of contesting taxes, particularly in its early years as exemplified by the Revolutionary War. Over the course of its history, however, the country has accepted taxation as a necessary means to fund conflicts and to share the burden of war with its citizens. Taxation funded the first three major conflicts in U.S. history: the War of 1812, the Civil War, and World War I.

The most poignant example of American wartime financial sacrifice took place during World War II, however. Facing the inexorable prospect of entering the struggle in Europe, the U.S. government committed to a dramatic overhaul of the nation's tax system to support the anticipated financial burdens of the looming conflict.[40] Less than one year following U.S. entry into World War II, Congress passed the Revenue Act of 1942, effectively expanding the federal income tax from a "class tax" to a "mass tax," a system that resembles today's tax structure.[41] The establishment of this fiscal sacrifice served as a profound departure from a long-standing aversion to government taxation of its citizens. Remarkably, however, approximately 90-percent of Americans surveyed deemed that the monetary sacrifice was fair.[42] Americans supported the nation's entry into World War II and did not shy away from personal sacrifice on behalf of the country.

---

[36] Ibid., 6.

[37] Ibid., 7.

[38] Friedman, "The Home Team."

[39] Maddow, *Drift*, 203.

[40] Steven A. Bank, Kirk J. Stark, and Joseph J. Thorndike, *War and Taxes* (Washington, DC: The Urban Institute Press, 2008), xiv.

[41] Ibid.

[42] Ibid.

America sustained the tradition of fiscal sacrifice during the Korean War, but this trend cooled notably during the Vietnam conflict when then President Johnson first balked and then reluctantly accepted an income tax surcharge to support t growing war costs. Three decades later, President George W. Bush enacted significant tax cuts just prior to the 9/11 attacks and the launch of became the longest war in American history. It seems remarkable, the, that in the months that followed, despite entering what appeared to be a lengthy conflict in Afghanistan, neither the administration nor Congress made any significant pleas for tax increases to fund military efforts. What proved even more astonishing and unprecedented were the subsequent tax cuts enacted in March 2003, just days after the U.S. military initiated the ground invasion of Iraq. In 2011, the Congressional Budget Office estimated that the cost of the Bush tax cuts totaled roughly $1.3 trillion in reduced government revenue, ironically almost the same cumulative cost of the wars in Iraq and Afghanistan through 2011.[43]

During the subsequent Obama administration, taxes remained low and, at times, decreased further. In fact, the average effective tax rate for all U.S. taxpayers ranged between 16.8 and 17.2-percent throughout the Bush and Obama administrations, with no increase in taxes to fund the post 9/11 wars.[44] In stark contrast, average tax rates during World War II and the Korean War rose sharply **to fund the nation's conflicts. Remarkably, the effective tax rate for a typical American rose from a** 1.5-percent in 1940 to 15.1-percent at the end of World War II, increasing federal revenues three-fold.[45] With decreased revenues from lower taxes, both the Bush and Obama administrations turned extensively to unparalleled financial borrowing from foreign nations to fund military operations in Afghanistan and Iraq.[46]

Instead of levying the responsibility to pay for the nation's wars on current generations, the Bush and Obama Administrations charted a dangerous course with two distinct and damaging outcomes. First, they effectively transferred the immense costs of the post-9/11 wars to future generations who cannot influence the current politica**l process thus removing the burden of paying for our nation's** wars from the current American populous. Second, by pursuing war funding via Continuing Resolution, the Executive branch practically circumvented the responsibility of budgetary oversight from Congressional control. In essence, Continuing Resolutions establish permanent appropriations that do not navigate traditional congressional appropriations processes, creating disincentives for Congress to provide effective oversight.[47] As a result, the government encouraged an already uninterested public to remain unengaged in U.S. foreign policy. With a diminished interest in and responsibility for overseeing the use of military spending, Congress further disengaged from decisions related to authorizing force, effectively deferring military matters to the Executive branch.

Future Implications

As the nation moves through the 21ˢᵗ century, several phenomena may strengthen the growing tendency to rely on the military to achieve foreign policy aims. First, the volatile and unpredictable

---

[43] Glenn Kessler, "Revisiting the Cost of the Bush Tax Cuts," *The Washington Post Online*, May 10, 2011, https://www.washingtonpost.com/blogs/fact-checker/post/revisiting-the-cost-of-the-bush-tax-cuts/2011/05/09/AFxTFtbG_blog.html?utm_term=.4f1d5c9ac262.

[44] Ritchie King, "Check your US Tax Rate for 2012 – and Every Year Since 1913," *Quartz Media LLC*, April 14, 2013, https://qz.com/74271/income-tax-rates-since-1913/.

[45] Bruce Bartlett, "The Cost of War," *Forbes*, November 26, 2009, http://www.forbes.com/2009/11/25/shared-sacrifice-war-taxes-opinions-columnists-bruce-bartlett.html.

[46] Harvey M. Sapolsky, "What Americans Don't Understand about Their Own Military," *Defense One*, May 6, 2015, http://www.defenseone.com/ideas/2015/05/what-americans-dont-understand-about-their-own-military/112042/.

[47] Jessica Tollestrup, *Automatic Continuing Resolutions: Background and Overview of Recent Proposals* (Washington, DC: Congressional Research Service, August 20, 2015), https://fas.org/sgp/crs/misc/R41948.pdf.

security environment is increasingly complicated by the rapid rise of non-state actors. Such entities do not respond in traditional ways to diplomatic, economic, or informational instruments of national power, which, in turn, fosters an increased likelihood of U.S. military interventions. Additionally, rising powers such as Russia and China are progressively contesting U.S. hegemony and the current state of global affairs. U.S. reactions may intensify the potential for conflict due opportunities for misperception and miscalculation, particularly if the U.S. continues to rely on the threat and military force at the expense of other instruments of national power.

A second factor that enables over-reliance on the military is the high regard that the public places in the armed forces. The U.S. military is arguably the best trained, educated, disciplined, and well-equipped force since the advent of the AVF. Naturally, Americans expect a high return on their investment. These high expectations, however, are further exacerbated by the increasing divide **between citizens and the military. This dynamic can be seen in the character of the nation's legislative** branch. Congress seems not to possess full appreciation for the military institution or its culture, is disinterested in conducting insightful or firm scrutiny over military matters.[48] Failure of the American public and Congress to maintain an unhealthy regard for the U.S. military is that they will not effectively scrutinize future military operations, further aggravating an over-reliance on American military might.

The final element supporting increased American military interventions is the rapid pace of technological advancements. Constant technological improvements over recent decades have **reinforced increased military operations and also intensified Americans' expectations for military** success. Unmanned platforms, precision weapons, and the prospects of autonomous weapons and **"super soldiers" expand U.S. military capabilities and promo**te a change to the character of war, where casualties and overall risk to U.S. military forces will be lower.

The promise of more swift and sterile conflicts will undoubtedly raise the public's expectations for military success and further reinforce a bel**ief that the "horrors of combat are things of the past."**[49] As a result, Americans may not comprehend the difficulties associated with future wars and acquiesce without critical and significant debate regarding U.S. military engaging in perilous operations. This **confluence of conditions increase the nation's vulnerability due to what prominent political journalist and author William Greider describes as "presumptions of unconquerable superiority," that will "lead** [the country] deeper and deeper into unwinnabl**e conflicts."**[50]

National Service

While the conditions that have allowed for an increasingly military-dominated American foreign policy may appear bleak, they can be remedied. The first step to better balance the use of the military is to instill in the citizenry a greater sense of service and commitment to the nation. Influential figures including General (Retired) Stanley McChrystal and U.S. Representative Charles Rangel who have advocated to re-institute a military draft in an effort to reinvigorate a service culture in American society and to extend the responsibilities of citizenship to a greater percentage of Americans.[51] Many, however, debate whether the cost of losing the professionalism and unparalleled efficacy of the All-

---

[48] Thompson, **"The Other 1%."**

[49] Karl W. Eickenberry and David M. Kennedy, "Americans and Their Military, Drifting Apart," *The New York Times Online,* May 26, 2013, http://www.nytimes.com/2013/05/27/opinion/americans-and-their-military-drifting-apart.html.

[50] William Greider, "The Fatal Flaw in American Foreign Policy," *The Nation*, September 4, 2014, https://www.thenation.com/article/fatal-flaw-american-foreign-policy/.

[51] Josh Rogin, "McChrystal: Time to Bring Back the Draft," *Foreign Policy*, July 3, 2012, http://foreignpolicy.com/2012/07/03/mcchrystal-time-to-bring-back-the-draft/.

Volunteer Force would outweigh the benefits of increased national service and sacrifice. In addition to promoting a return of the military draft, Representative Rangel also encouraged implementing and expanding national service programs as a way to minimize the costs and extend benefits of American freedom as widely as possible.[52]

Rangel's Universal National Service Act proposed mandatory registration for selective service and two years of compulsory service for all citizens between the ages of 18 to 25.[53] Men and women could fulfill their obligation in any number of occupations and agencies such as schools, hospitals, **airports, or military service. Rangel's proposal sought to ensure that** "all Americans are involved in our defense [and that] every family will fully engage in any decision **to use force."**[54]

Several other notable figures (e.g., Hillary Clinton and Senator John McCain) have proposed similar mandatory service programs, although none of the recommendations gained significant traction in Congress. Incentivizing, rather than mandating national service may be a more feasible approach for garnering increased investment and sacrifice from Americans. General McChrystal recently called for such incentive programs, proposing that the nation encourage colleges and corporations to promote **national service. His idea envisions the government incentivizing "schools** [to] adjust their acceptance policies and employers their hiring practices to benefit those who have **served."**[55] Ultimately, any measure the nation adopts to inculcate greater commitment and sense of service should strengthen participation in the political process and intensify debate on the appropriate use of military force.

Narrowing the Civil-Military Gap

The civil-military gap will continue to widen as the U.S. population grows. The nation must, however, undertake meaningful efforts to gain improved military representation from across the nation to reconnect society with its military. The U.S. can first begin by rebalancing ROTC programs, particularly in the Northeast and in the largest urban areas. Fortunately, the military has already begun to address this issue. In 2013, U.S. Army Cadet Command announced that it would be closing 13 ROTC programs to shift financial resources to 56 different markets, to include Los Angeles, New York, and Chicago.[56]

Additionally, Cadet Command expanded scholarship opportunities to recruit students from inner-**cities, announcing an urban scholarship initiative to better reflect the "geographic and demographic diversity of the country."**[57] While ongoing movements to rebalance officer recruitment from across the nation are essential, the military must also gain better geographic representation for its enlisted population. To accomplish this, the military must expand recruitment efforts beyond the historically strong South and West regions. Creating a more geographically representative force is a vital step to more effectively binding the public to the military while ensuring expanded public engagement and debate on future decisions to use force.

---

[52] **Charles Rangel, "All Americans Have a Duty to Defend our Nation,"** *USA Today Online*, February 15, 2013, http://www.usatoday.com/story/opinion/2013/02/15/two-years-compulsory-service-rangel/1922597/.

[53] Ibid.

[54] Ibid.

[55] Conor **Friedersdorf, "The Case against Universal National Service,"** *The Atlantic*, June 26, 2013, https://www.theatlantic.com/politics/archive/2013/06/the-case-against-universal-national-service/277230/.

[56] **Alan Binder, "R.O.T.C. Making Cuts to Expand Recruiting,"** *The New York Times Online,* October 21, 2013, http://www.nytimes.com/2013/10/22/us/making-cuts-to-expand-recruiting-for-rotc.html?_r=0.

[57] **Vickey Mouze, "New Army ROTC Scholarships Anticipate Future Leadership Needs,"** *Army Online*, September 27, 2013, https://www.army.mil/article/112298/New_Army_ROTC_scholarships_anticipate_future_leadership_needs.

Reform the War Powers Resolution

The Constitution clearly states that Congress has the prerogative to authorize a non-defensive war, a power that it has increasingly failed to assert. Although Congress passed the 1973 War Powers Resolution to affirm its control over war-making decisions, in practice, this law has failed to curb the Executive. In fact, no president has recognized the constitutionality of the War Powers Act and recent **presidents have blatantly ignored Congress's role in authorizing the use of force.** To complicate matters further, **the resolution's 60**-day limit on committing military force for hostilities without congressional approval has proven to be a critical flaw.[58] This stipulation, in effect, recognizes the **president's ability to unilaterally engage** in war-making. Furthermore, the 60-day limit strongly ties the hands of the Legislative branch as options to recall forces once deployed are often severely limited by political pressures.

Recently, efforts have emerged in both the House and the Senate to reform the War Powers Resolution. U.S. Representative Chris Gibson recommended a 48-hour requirement for the President to report to Congress following any introduction of armed forces into hostilities, repealing the existing 60 and 90-day timelines.[59] Senators John McCain and Tim Kaine proposed reducing the period where the President could commit military forces to seven days before both houses of Congress would vote to authorize continued military operations.[60] Neither of the proposed amendments is sufficient, however. The previous two administrations liberally applied the 2001 Congressional Authorization for the Use of Military Force in Response to the 9/11 attacks to justify military actions world-wide, far beyond the scope of the original authorization. Moreover, Congress has repeatedly demonstrated an unwillingness to countermand the Executive once military forces are employed. The War Powers Resolution must be amended to require congressional approval prior to the deployment of the military short of the immediately necessary national defense, as the Founding Fathers envisioned.[61] Furthermore, due to the increased role of non-state actors and frequent U.S. counter-terrorism campaigns, any amendment to the War Powers Resolution must insist upon a very strict definition of war to prevent the Executive from taking advantage of ambiguous situations where conflict may result.[62]

Funding Future Military Actions

The aforementioned proposals are meaningful remedies that can help the country re-balance its use of the military with the other instruments of national power. The most effective measure the nation must take, however, is to change the manner in which it finances war. Taking action to ensure that American citizens share in the burdens of war would force a much needed and long-overdue debate concerning when and where the military should be employed. The current practice of transferring the costs of war onto future generations is a troubling development.[63] Increasing taxes or reducing government benefits or consumption are all practical approaches to more appropriately **fund the nation's wars. To solidify this remedy and to fundamentally change how America funds its**

---

[58] Center for Constitutional Rights, *Restore. Protect. Expand. Amend the War Powers Resolution* (New York: Center for Constitutional Rights, 2009), 1, https://ccrjustice.org/sites/default/files/assets/CCR_White_WarPowers.pdf.

[59] H.R. 560 – War Powers Reform, 114th Congress, January 27, 2015, https://www.congress.gov/bill/114th-congress/house-bill/560, referred to the Committee on Foreign Affairs.

[60] **Ramsey Cox, "Senate Bill Amends War Powers Act,"** *The Hill*, January 16, 2014, http://thehill.com/blogs/floor-action/senate/195704-senate-bill-amends-war-powers-act.

[61] Bacevich, *The New American Militarism*, 210.

[62] **Friedman, "The Home Team."**

[63] **Sapolsky, "What Americans Don't Understand About Their Own Military."**

wars, Congress must pursue legislation that prohibits military deployments to conflicts without an established and approved funding source.

Representative Gibson's (R-NY-19) offered House Resolution 560 lays out a feasible course for **paying for future wars. His proposal prohibits funds "from being obligated or expended for** introducing the Armed Forces into hostilities, or into situations where imminent involvement in hostilities is clearly indicated, in the absence of (1) a declaration of war; (2) specific statutory authorization; or (3) a national emergency created by an attack or imminent threat of attack upon **the United States, its territories or possessions, or the Armed Forces."**[64]

The unwillingness of the Bush and Obama administrations to raise taxes to fund the wars in Iraq and Afghanistan may be linked to fading public support. Admittedly, raising taxes or reducing government spending remains a controversial topic in Washington. Yet, if America is to re-balance its use of the military with other instruments of national power, it must be willing to re-examine both how and how much it funds military actions. By tethering future military actions to approved funding, the nation would force its citizenry and Congress to re-engage with the political process and decide whether the stakes of proposed military actions are worth the cost.[65] America would be wise **to follow John F. Kennedy's advice and be prepared to "pay any price, bear any burden, meet any hardship" to wage war or, alternatively, to find another solution.**[66]

Conclusion

America finds itself far removed from the nation that reluctantly entered, yet strongly supported World Wars I and II, where the country largely mobilized, maintained tight connections between the citizenry and the military, and exercised sustained sacrifice. As the civil-military divide has grown, both the public and Congress have largely abdicated their responsibilities in the political process for determining the role of the U.S. military. Additionally, both the Legislative and Executive branches have progressively failed to ensure citizen involvement and sacrifice in support of the **nation's wars.** The consequence of these failures is an empowered Executive branch that frequently and with increasing regularity employs the armed forces as the primary instrument of national power responsible for advancing and protecting national interests.

Despite these alarming trends, America can return to conditions more closely aligned with the original views of the Framers. Pursuing national service programs and developing a more geographically representative military will decrease the civil-military gap and better connect Americans with their military. Generating greater constituent participation should result in improved congressional oversight on military activities, reinforced by a strengthened War Powers Resolution. Furthermore, ensuring that Americans sacrifice financially via war taxes or reduced government spending or consumption will further solidify their participation in the political process.

U.S. military operations remain vital to preserving national security or fighting tyranny. America must reinvigorate deliberative processes to decide when and where to use military force, and in doing so, ensure that both its citizens and Congress are active participants. Such measures should assist the nation in better implementing all instruments of national power in support of foreign policy **pursuits while simultaneously returning America to a closer alignment with the Founders' intent.**

---

[64] H.R. 560 – War Powers Reform, 114th Congress, January 27, 2015, https://www.congress.gov/bill/114th-congress/house-bill/560.

[65] R. Russell Rumbaugh, "A Tax to Pay for War," *The New York Times,* February 10, 2013, http://www.nytimes.com/2013/02/11/opinion/a-tax-to-pay-for-war.html.

[66] Bartlett," The Cost of War."

The Great Enabler: The AVF and the Use of Force

Scott W. Mueller

America's All-Volunteer Force (AVF) is a highly-debated concept in the realm of U.S. civil-military relations. While the quality of today's AVF is rarely disputed, some question whether or not it has led to a too-frequent use of American military force. The argument advanced here is that the American AVF enables the use of military force as a foreign policy instrument, but not for the reasons laid out by the 1973 Gates Commission. With the return to the AVF in 1973, Congress and America's military leaders took steps to prevent U.S. presidents from embarking on military adventures. However, the tendency of U.S. presidents to use military force to resolve foreign policy disputes that are not vital to the national interest is enabled by the AVF. Moreover, the AVF is essential to maintaining the liberal international order.

Keywords: *All-Volunteer Force, Military Adventurism, Conscription, Military Manpower System*

Conscription is the taproot of militarism and war.

—Jan Smuts[1]

The continuing war in Vietnam figured prominently into the 1968 presidential campaign. Into its third year and after the shock of the Tet Offensive, the war was exceptionally unpopular and appeared to be a losing proposition. Protests against the war raged across the United States with the draft as a particular target of disdain. In his bid for the presidency that year, Richard Nixon promised to end the draft if elected. He fulfilled that promise in 1973 when the United States ended the draft and returned to a military comprised entirely of volunteers.

The All-Volunteer Force (AVF) has since been a highly-debated concept in the realm of civil-military relations. While the quality of today's AVF is rarely disputed, some question whether or not

---

[1] Jeffery Pickering, "Dangerous Drafts? A Time-Series, Cross-National Analysis of Conscription and the Use of Military Force, 1946-2001," *Armed Forces & Society* 37, no. 1 (Winter 2011): 120-121, quoted from Denis Hayes, *Conscription Conflict: The Conflict of Ideas in the Struggle for and against Military Conscription in Britain between 1901 and 1939* (New York: Garland, 1973), 346.

it has led to a too-frequent use of American military force. This concern was specifically addressed by the commission established by President Nixon to study the feasibility and impacts of returning **to an AVF, and the President's Commission on an All**-Volunteer Armed Force (the Gates Commission) concluded that this concern was unjustified. Recent history, however, suggests otherwise.

With the establishment of the Clinton Doctrine in the 1990s, the United States embarked on a number of military operations for reasons other than the preservation of national sovereignty. The strongest advocates for the use of military force, however, have been civilian policy makers—not a **military elite as stated in the concerns addressed by the Gates Commission. Thus, America's AVF has** enabled the use of military force as an instrument of foreign policy, though not necessarily for the reasons laid out by the Gates Commission.

The AVF is not a new concept in American history, rather it is grounded in tradition and moral philosophy. After a discussion of the Gates Commission findings on the AVF, I show how Congress **and America's military leaders took steps to prevent presidents from embarking on military** adventures. Yet despite these efforts, American presidents, especially in the 1990s, were able to emplo**y the AVF for reasons not always critical to the country's vital interests.** Finally, I conclude that the AVF, while enabling the use of military force, is an essential system that allows the United States **to stand as the world's guardian of the liberal int**ernational order.

Resurrecting the All-Volunteer Force

Throughout its history, the United States has alternated between conscript and volunteer military manpower systems. **Possessing a distrust of standing armies, the country's founders relied** on volunteers in the state militias and the federal armed forces for the defense of the nation. Some of **the nation's founders were concerned that a standing army would encourage the use of force to settle** international disputes.[2] Geography played a large role as well: protected from the rest of the world by two oceans and a huge frontier, the United States did not need a large army like those common in Europe at the time.[3] As a result, the United States from its founding maintained a small military force focused on expanding the country westward, protecting territorial outposts, and securing its overseas **commerce to help fuel the growing nation's economy.** Quality within this AVF suffered greatly, however, as the U.S. military had to compete for recruits with an ever-expanding economy.[4] This **AVF nevertheless satisfied the young country's needs for a time.**

The scope and scale of industrial warfare, however, demanded that the United States rely on conscription to raise the massive armed forces that fought in the American Civil War, World War I, and World War II. **This departure from American military tradition was "rationalized on the grounds** that the rights guaranteed to the individual by the government implied an obligation upon him to defend his rights by defending the gove**rnment that assured them."[5] With the nation's survival and** vital interests at stake, the idea of conscription on moral grounds was, for the most part, widely accepted by the American public. The United States returned to volunteerism when those conflicts

---

[2] John Whiteclay Chambers et al., eds., *The Oxford Companion to American Military History* (Oxford: Oxford University Press, 1999), 595.

[3] James S**heehan, "The Future of Conscription: Some Comparative Reflections," in** *The Modern American Military*, ed. David M. Kennedy (New York: Oxford University Press, 2013), 178. The author quotes Alexis de Tocqueville who wrote that **Americans have "no neighbors, and consequently they have no great wars...nor great armies, nor great generals." Alexis de** Tocqueville, *Democracy in America* (New York: Everyman's Library, 1994), 288-289.

[4] Chambers, *The Oxford Companion to American Military History*, 594-595.

[5] Ibid.

ended and the threats subsided. Communism continued its march across Eastern Europe and China, however, and in 1948 Congress again resorted to conscription to defend the nation. This draft remained in place until 1973, providing the military manpower to fight most notably in Korea and Vietnam. **But during the Vietnam War, conscription's legitimacy as a military manpower system** became a heated point of contention in American society.

The Vietnam War—**America's longest armed conflict until the post**-911 campaigns in Iraq and Afghanistan—became increasingly unpopular in the United States beginning in 1966 when the anti-war movement blossomed into mass protests.[6] This popular movement had a particular dislike for the draft. Burning draft cards and avoiding military service (either through education deferments, joining the National Guard or reserves, or refusing to register for the draft) became popular forms of civil disobedience. Not since the New York City draft riots in July 1863 had conscription been opposed so vociferously, and certainly not on such a large scale as seen during the Vietnam War. Counter to the pre-established ideals of civic duty, the anti-war movement viewed the Vietnam War **draft as the government's infringing on citizens' rights by forcing cons**cripts to fight a war they did not support against an enemy that did not pose an existential threat to the United States.[7] Rhodes Scholar (and future 42nd President of the United States) Bill Clinton articulated this idea in a 1969 letter to the professor of military science at the University of Arkansas Reserve Officer Training Corps program:

> From my work I came to believe that the draft system itself is illegitimate. No government really rooted in limited, parliamentary democracy should have the power to make its citizens fight and kill and die in a war they may oppose, a war which even possibly may be wrong, a war, which, in any case, does not involve immediately the peace and freedom of the nation.[8]

This intense opposition to the draft and the Vietnam War propelled Richard Nixon to the presidency in the 1968 elections with his promise to end the draft. In 1970, he established The **President's Commission on an All**-Volunteer Armed Force to study the issue and make recommendations.

The President's Commission on an All-Volunteer Armed Force

On March 27, 1969, fulfilling one of his presidential campaign pledges from the 1968 presidential race, President Nixon announced the appointment of an Advisory Commission on an All-Volunteer Force chaired by former Secretary of Defense Thomas S. Gates. The purpose of the Gates Commission **(as it came to be known) was to "develop a comprehensive plan for eliminating conscription and** moving toward an all-**volunteer armed force."**[9] The fifteen-member commission consisted of prominent businessmen, scholars, economists, a former Supreme Allied Commander-Europe, and the Executive Director of the National Association for the Advancement of Colored People (NAACP).[10] The commission submitted its final report to President Nixon on February 20, 1970,

---

[6] Ibid., 764.

[7] James Burk, "The Changing Moral Contract for Military Service," in *The Long War: A New History of U.S. National Security Policy Since World War II*, ed. by Andrew J. Bacevich (New York: Columbia University Press, 2007), 442.

[8] **"Bill Clinton Letter to Colonel Eugene Holmes,"** *PBS,* December 3, 1969, http://www.pbs.org/wgbh/pages/frontline/shows/clinton/etc/draftletter.html. In his letter, to Colonel Holmes, Clinton **stated he was "working every day against a war I opposed and despised with a depth of feeling I had reserved solely for racism in America before Vietnam."**

[9] Thomas S. Gates, *President's Commission on an All-Volunteer Force* (Washington, DC: Library of Congress, 1970), vii.

[10] Ibid., viii-ix. Members included Milton Friedman, Alan Greenspan, Alfred Gruenther (former SACEUR), and Roy Wilkins (Executive Director of the NAACP).

stating: "We unanimously believe that the nation's interests will be better served by an all-volunteer force, supported by an effective stand-by draft."[11] The commission's conclusions sounded the death knell for the draft that had fueled so much public discontent. The report was also significant because while the United States was returning to the AVF, the dissolution of the draft committed the country to maintaining a large military force comprised solely of volunteers.[12] America's historic suspicion of standing armies and military adventurism once again came to the fore, demanding that the Gates Commission address concerns about potential effects of returning to the AVF.

The Gates Commission considered nine separate "objections" to the AVF that arose. One objection, and the focus of this paper, was that "[a]n all volunteer force would stimulate foreign military adventures, foster an irresponsible foreign policy, and lessen civilian concern about the use of military forces."[13] According to this argument, the AVF would encourage military adventurism because of three "important inferences: (1) an all-volunteer force will be more aggressive than a mixed force; (2) the nation's civilian and military leaders will risk the lives of volunteers with less concern than those of conscripts and (3) a questionable foreign commitment could be undertaken and sustained with less popular dissent than if conscripts were used."[14]

The commission, however, believed this objection to be unfounded. First, according to the commission, the military manpower system was irrelevant in deciding to use military force. The commission acknowledged existing pressures to use conscripted military force to solve foreign policy problems, and this would not change with the AVF. The nation's leadership would still have to weigh the cost in blood and treasure as well as domestic and foreign political costs before committing a conscript, blended, or AVF to a conflict. The president also had to weigh the possibly that any substantial commitment of military power could risk potential nuclear conflict with the Soviet Union. Finally, the commission argued the size and readiness (two important military factors considered during decisions to use military force) of the U.S. military would remain unchanged under either the AVF or the current mixed system of conscripts and volunteers. The main difference would be that under the mixed system, the President could independently increase draft calls to expand the size for the force (as President Johnson did during the Vietnam War). Under an AVF, however, the President would have to ask Congress to enact the standby draft and conscription. This request would then theoretically spark a national debate and public discussion on the necessity of employing military power and would only be used if supported by the American public.[15]

The Gates Commission also addressed the concern that an AVF would reduce the American public's interest in foreign affairs because fewer Americans would be called upon to serve. A general lack of foreign affairs interest would dilute the national debate about enacting the standby draft and diminish the effect of public opinion as a hedge against military adventurism. The commission stated that higher education levels, friendship and familial relations with service members, "the diffusion of mass communications, and the newsworthiness of compelling national security interests" would retain the public's interest in how the United States utilized the AVF.[16] The commission also

---

[11] Ibid., iii.

[12] Louis G. Yuengert, "America's All Volunteer Force: A Success?" *Parameters* 45, no.4 (Winter 2015-2016): 55.

[13] Gates, *President's Commission on an All-Volunteer Force, 17.*

[14] Ibid., 156. The mixed force of volunteers and conscripts was the military manpower system in place at the time of the commission's study and report.

[15] Ibid., 17-18.

[16] Ibid., 156. "The claim is made that the ranks of the public attentive to foreign policy are swelled significantly by those citizens touched by the draft. It is a doubtful notion. The corollary—that public interest in foreign affairs will decrease significantly if volunteerism is adopted—is also doubtful. Volunteers have as many concerned relatives and friends as men who are drafted. Higher education levels, the diffusion of modern mass communications, and the newsworthiness of

concluded that the AVF would make explicit the cost of using military force, thereby retaining the interest of American taxpayers whose tax dollars would have to finance the endeavor, especially if expanding the AVF should become necessary.[17]

Finally, conscription advocates were concerned that this new AVF would violate one of America's most fundamental principles: civilian control of the military. AVF detractors argued that the AVF would be better trained and equipped and, therefore, more aggressive; it would have a higher degree of autonomy from the civilian leadership, and the AVF's military leadership would exploit international crises for its own gain.[18] This argument suggested military leaders would actively seek to employ military force because there would be no point to having a professional, highly trained and well equipped force unless it was to be used. The commission concluded this objection was irrational: they were advocating a change to the country's military manpower system, not the political authorities and processes that governed the use of the military instrument of power.[19]

In the end, the Gates Commission concluded that objections to the AVF based on fears associated with military adventurism in U.S foreign policy were unfounded:

> We have examined how the return to volunteer forces might affect the decision to use U.S. military power. We conclude that the recommended all-volunteer force will actually increase democratic participation in decisions concerning the use of military force. We reject the fear of increased military aggressiveness or reduced civilian concern following the return to an all-volunteer force.[20]

President Nixon accepted the Gates Commission's recommendations. In 1973, Secretary of Defense Melvin Laird announced the formation of the All-Volunteer Force, thus ending conscription as America's military manpower system for the previous 25 years. The commission's rebuttals to the objection that the AVF would lead to military adventurism, however, proved not to be entirely accurate, as did the reasoning behind the objection that a professionalized AVF would instigate military adventurism. In the decades following the return to the AVF, it was not the resultant professionalized military that would encourage use of the military instrument to solve foreign policy issues. With the specter of Vietnam still fresh in the minds of civilian and military policymakers, the Congress and Defense Department leaders sought to limit military force as the foreign policy tool of choice, and thus prevent military adventurism.

Hedges against Military Adventurism

One objection to the AVF was that a president and his military leaders would be more apt to use military power as the nation's foreign policy tool of choice. With fewer Americans serving in the military the vast majority of the American public would lose interest in foreign affairs and would not care about the President committing volunteers to conflicts across the globe. Congress, however, did not completely subscribe to the Gates Commission's logic on why the AVF would not enable a President to engage in military adventurism. The Congress wanted to ensure that the "collective judgement of both the Congress and the President will apply" prior to committing U.S. forces into

compelling national security events assure that foreign affairs will hold the attention of a substantial and growing public, regardless of the method used for procuring military manpower."

[17] Ibid., 155.
[18] Ibid., 157.
[19] Ibid.
[20] Ibid., 155.

hostilities, in accord with the intent of the Constitution's framers.[21] In 1973 Congress passed the War Powers Resolution (over President Nixon's veto), requiring:

> The President in every possible instance shall consult with Congress before introducing United States Armed Forces into hostilities or into situations where imminent involvement in hostilities is clearly indicated by the circumstances, and after every such introduction shall consult regularly with the Congress until United States Armed Forces are no longer engaged in hostilities or have been removed from such situations.[22]

Most importantly, the resolution allowed the President only 60-90 days in which to cease using U.S. troops unless Congress authorized their use or extended the timeframe.[23] Another hedge against military adventurism came from the Department of Defense in the form of the Weinberger and Powell Doctrines.

Secretary of Defense Caspar Weinberger (1981-1987), in a 1984 speech to the National Press Club, articulated the conditions which he believed must be met before using military force. The Weinberger Doctrine called for committing U.S. military forces to combat only for reasons of vital national interests and only if the nation was committed to winning. Weinberger insisted that the nation's political and military leadership clearly define the political and military objectives, and commit enough forces to accomplish those objectives. He also required "reasonable assurance we will have the support of the American people and their elected representatives in Congress," and that the nation's leaders candidly articulate to the American people and Congress the threat and reasons for using force. Finally, the United States should only use force as a last resort. The Weinberger Doctrine's six criteria were "intended to sound a note of caution—caution that we must observe prior to committing forces to combat overseas."[24] While serving as the Chairman of the Joint Chiefs of Staff from 1989-1993, General Colin Powell invoked the Weinberger Doctrine advising President George H.W. Bush on the use of military force to expel Saddam Hussein's forces from Kuwait in 1990. General Powell added to the doctrine, however. The resultant Powell Doctrine insisted the United States use overwhelming force whenever committing forces to combat.[25]

The War Powers Resolution, the Weinberger Doctrine, and the Powell Doctrine all have roots in the tumultuous American political and military experience in Vietnam. They sought to curb the executive branch's ability to commit U.S. troops to combat without an appropriate national debate, but especially out of concern that the return to the AVF would enable Presidents to use force as the foreign policy tool of first resort. In practice, however, the War Powers Resolution and Weinberger and Powell Doctrines have been only mildly successful. The War Powers Resolution, deemed unconstitutional by every president from Nixon to George W. Bush,[26] is only invoked by Congress when disagreement arises among the elite (the president, politicians, media, intellectuals, national security experts) as to whether or not military force is the proper answer to a foreign policy issue.[27] From 1975 to March 2015, U.S. presidents submitted 160 reports to Congress in accordance with the

---

[21] *The War Powers Resolution of 1973*, Public Law 93-148, 87 Stat. 555, 93rd Cong., 1st sess. (November 7, 1973), https://www.law.cornell.edu/uscode/text/50/1541.

[22] Ibid.

[23] Ibid.

[24] Caspar Weinberger, "The Uses of Military Power," public speech, The National Press Club, Washington, DC, November 28, 1984, http://www.pbs.org/wgbh/pages/frontline/shows/military/force/weinberger.html.

[25] Chambers, *The Oxford Companion to American Military History*, 556.

[26] Matthew C. Weed, *The War Powers Resolution: Concepts and Practice* (Washington, DC: U.S. Library of Congress, Congressional Research Service, April 3, 2015), i.

[27] Gregory P. Noone, "The War Powers Resolution and Public Opinion," *Case Western Reserve Journal of International Law* 45, no. 1/2 (Fall 2012): 145.

War Powers Resolution. And while Congress authorized the use of force in 1991 and 2002 against Iraq, presidents and Congress have little appetite "to initiate the procedures of or enforce the directives in the War Powers Resolution."[28] Generally, Congress is willing to let the President use military force without interfering as politicians do not want to appear to not "support the troops" given that the U.S. military is so highly regarded by the American people.[29] The War Powers Resolution has, however, shaped the way presidents use military power, preferring action that is limited in duration of 60-90 days so that they do not have to submit reports to Congress. The War Powers Resolution has therefore not constrained presidential use of force as a foreign policy instrument. Arguably, the military elites have been the most reluctant to use the military instrument of national power, and probably none more so than General Colin Powell.

As Chairman of the Joint Chiefs of Staff, Colin Powell was concerned about using the military to advance U.S. values when national interests were not at stake. In contrast to the 1991 Gulf War where Iraq invaded a sovereign country and gained control of significant sources of oil, the efforts in Haiti, Somalia, Bosnia, and Kosovo injected the United States into the internal issues of those countries. The Clinton Administration sought to use military force for nation building in these countries despite lack of an existential threat to the United States.[30] General Powell's concern stemmed from the fact that these missions did not adhere to the Powell Doctrine because of a lack of coherent objectives and limitations placed on the military did not enable the overwhelming military force.[31] More recently, during the debates to use military force to invade Iraq and depose Saddam Hussein in 2002, retired General Anthony Zinni was an outspoken critic of the Bush Administration's desire to invade Iraq: "It's pretty interesting that all the generals see it the same way and all the others who have never fired a shot and are hot to go to war see it another way."[32]

Research by Peter Feaver and Christopher Gelpi reveals that civilian elites with no military experience are more likely to use force, albeit in more limited ways, than military elites. A now-famous exchange between the United States' Ambassador to the United Nations, Madeline Albright and Chairman of the Joint Chiefs General Colin Powell during debates within the new Clinton Administration on employing military force illustrates this point. Ambassador Albright, frustrated by General Powell's adherence to the Weinberger and Powell Doctrines, asked General Powell: "What is the point of having this superb military that you're always talking about if we can't use it?"[33] Senate Republican Leader Trent Lott remarked during the 2002 debates on the Iraq invasion: "If the military people don't want to fight, what is their role? Do they want to be people that clean-up after natural disasters?"[34] Concerns that the AVF would give rise to a military so disconnected from society that military leaders would actively seek to use the military instrument have proven false, but not because civilian leaders have prevented it. On the contrary, the United States' civilian leadership advocates for the use of military force more than military elites. Contrary to the Gates Commission's

---

[28] Weed, *The War Powers Resolution: Concepts and Practice*, i. For a complete listing of WPR reporting instances, see pages 59-88.

[29] Noone, "The War Powers Resolution and Public Opinion," 151. According to Noone's research, the American public overwhelmingly supports the military during times of conflict and politicians are very attuned to this.

[30] Michael Mandelbaum, *Mission Failure: America and the World in the Post-Cold War Era* (Oxford: Oxford University Press, 2016), 368.

[31] Peter D. Feaver and Christopher Gelpi, *Choosing Your Battles: American Civil-Military Relations and the Use of Force* (Princeton, NJ: Princeton University Press, 2004), 6.

[32] Ibid., 1. Quoted from Mike Salinero, "Gen. Zinni Says War with Iraq is Unwise," *Tampa Tribune*, August 24, 2002, 1.

[33] Ibid., 2. Quoted from Colin Powell with Joseph E. Persico, *My American Journey* (New York: Ballantine, 1995), 576-577.

[34] Ibid., 3. Quoted from Bill Gertz and Rowan Scarborough, "Inside the Ring," *Washington Times*, October 11, 2002, 10.

arguments that the AVF would not lead to military adventurism, the AVF has seemingly enabled a more active use of force by the United States.

The All-Volunteer Force and the Application of U.S. Military Power

The AVF is not a new or revolutionary concept in America; it has, in fact, been the norm throughout the vast majority of the country's history. To say that the modern AVF has led to military adventurism in U.S. foreign policy is also a fallacy. By most counts American presidents have used force abroad over 300 times since the country's founding.[35] According to retired lieutenant general and former Ambassador to Afghanistan Karl Eikenberry, half of those "conflict-related military deployments" occurred after World War II; from 1946-1973, the United States conducted 19 overseas deployments, but 144 overseas deployments from 1973-2012 during the modern AVF.[36] These figures are often cited to show that the modern AVF has contributed to military adventurism since 1973. The notion that an AVF leads to more frequent uses of force is also grounded in Kantian philosophy. Kant argued conscript armies in a republic link the people with their national leadership. They will, therefore, be "very cautious of decreeing for themselves all of the calamities of war."[37] This sentiment was also expressed by U.S. Representative Charles Rangel in 2006 when he advocated for a return to conscription: "Decision makers...would more readily feel the pain of conflict and appreciate the sacrifice of those on the front lines if their children were there too."[38] Research suggests, however, that conscripted militaries may not be the hedge against military adventurism as conscription advocates believe.

Professor Jeffrey Pickering indicates that nations with conscription as their military manpower system are more likely to use military force than nations with an AVF system.[39] Pickering found that the probability that states with conscription will use "belligerent military force" is 58 percent higher than states with AVFs. These states are also 39 percent more likely to engage in operations other than war, and have a 227 percent higher probability of using force against non-state actors than do states with AVFs. His research also found that military manpower systems have no impact on a nation's decision to deploy military forces for humanitarian missions. In those instances, leaders only deploy their forces when they are confident that the risk to their soldiers' lives is exceptionally low. More so than the military manpower system, a nation's military capabilities play a larger role in determining whether or not a nation will use military force. The more capable the force, the more likely that force will be employed.[40] Pickering makes a compelling argument backed by statistical modeling, whereas conscription advocates rely on moral and philosophical arguments. What is not clear from his research, however, is the context within which the nations he studied employed military force, and to what degree their military manpower systems played a role in the decision to use force vice the need to protect vital national interests. Also, he does not clearly stipulate the form of government utilized by the nations examined. It stands to reason that dictatorships with conscript armies and suppressive regimes care less about public opinion and political consequences than do democratic

---

[35] Ryan C. Hendrickson, *The Clinton Wars: The Constitution, Congress, and War Powers* (Nashville, TN: Vanderbilt University Press, 2002), 1.

[36] Karl W. Eikenberry, "Reassessing the All-Volunteer Force," *The Washington Quarterly* 36, no.1 (Winter 2013): 10, http://dx.doi.org/10.1080/0163660X.2013.751647.

[37] Pickering, "Dangerous Drafts? A Time-Series, Cross-National Analysis of Conscription and the Use of Military Force, 1946-2001," 120, quoted from Immanuel Kant, *Immanuel Kant's Political Writings*, ed. Hans Reis, ed., translated by H.B. Nesbit (Cambridge, UK: Cambridge University Press, 1963), 94.

[38] Ibid., 120.

[39] Ibid., 119.

[40] Ibid., 129-131.

republics. Saddam Hussein and the Iran-Iraq War is a case in point. World order standing or placement likely has an impact on how nations use military force. The **United States, as the world's** lone superpower in the post-Cold War world, has a vital interest in maintaining the liberal international order that influences how and where it uses military force.

The United States is arguably more likely to use military force than other nations given its place in the world. The United States emerged from World War II as a superpower and the leader in the effort to stem the tide of international communism. With the fall of the Soviet Union, the United States assumed the mantle of preserving the liberal international order and used its military power—the highly capable and professional AVF—to protect that international order, protect its vital national interests, and promote national values.[41] To do this, the United States at times has used force either as a deterrent to aggression by an adversary or as a means by which to compel an adversary to conform to the international order. The AVF enables the use of military force because it frees political leaders from the constraints inherent to conscription as a military manpower system: namely a citizenry that resists conscription when vital interests are not at stake. The first Chancellor of the **German Empire Otto von Bismarck put it succinctly when he stated, "Conscripts cannot be** sent to **the tropics."**[42] While the United States has no colonies to police as did the European powers of the 19th and early 20th centuries, the maintenance of the liberal international order has become **Bismarck's "tropics" for the United States in late**-20th and early 21st centuries. And while the United States has used its AVF as an instrument of foreign policy throughout the world in the maintenance of the international order, the American people have not completely ceded their role in the debate on with regard to when and how force should be used.

Much of the literature surrounding the AVF focuses on the civic duty of a republic's citizenry to participate in the collective defense of the country and the ways this has been diminished by the AVF in the United States. **Ambassador Karl Eikenberry falls into this camp, stating: "We collectively claim** the need for a robust armed forces given the multi-faceted foreign threats our country faces, and yet as individuals, do not wish to be troubled with any personal responsibility for manning the **frontier."**[43] Andrew Bacevich, a prominent critic of the AVF, believes that American political elites **"neither seek nor seriously consider the views of the larger public"** concerning foreign policy and the use of military force, an**d that "most citizens dutifully accept their exclusion from such matters."**[44]

The American public, however, has demonstrated that it remains interested and informed about **its government's use of military power.** Public outrage over American casualties in the 1983 Marine barracks bombing in Beirut, the 1993 Battle of Mogadishu in Somalia, and the raging insurgency in Iraq in 2006 forced presidents to withdraw forces (as in Beirut and Somalia) or to bring in fresh leadership and adopt a new strategy (hence the Iraq Surge and counterinsurgency doctrine).[45] The **American public's frustration over the war in Iraq was a key factor in electing Barack Obama to the**

---

[41] Barack Obama, *National Security Strategy* (Washington, DC: The White House, February 2015), 2. See pages 19-23 for national values and the international order.

[42] Sheehan, "The Future of Conscription: Some Comparative Reflections," 179.

[43] Eikenberry, "Reassessing the All-Volunteer Force," 39.

[44] Andrew J. Bacevich, "The Elusive Bargain: The Pattern of U.S. Civil-Military Relations Since World War II," in *The Long War: A New History of U.S. National Security Policy Since World War II*, ed. by Andrew J. Bacevich (New York: Columbia University Press, 2007), 208.

[45] For Somalia, see David P. Auerswald and Peter F. Cowhey, "Ballotbox Diplomacy: The War Powers Resolution and the Use of Force," *International Studies Quarterly* 41, no. 3 (September 1997): 522.

For Beirut, see Andrew J. Bacevich, *America's War for the Greater Middle East: A Military History* (New York: Random House, 2016).

See also Glenn P. Hastedt, *American Foreign Policy: Past, Present, and Future*, 10th ed. (Lanham, MD: Rowan and Littlefield, 2014), 181-183.

presidency in 2008 along with his campaign promise to end the war there. Public sentiment also profoundly influenced his operational approach to destroying the Islamic State in Iraq and Syria (ISIS) in 2014. **President Obama's belief that the American public would not support another ground** war in that region led to a strategy and operational approach that relied on U.S. and coalition airpower and intelligence capabilities in support of proxies fighting ISIS on the ground.[46]

These examples indicate that Americans have not divorced themselves from the debate on the use of military force simply because they have **less "skin in the game" due to the AVF.** They are still part of the equation and continue to shape the character of the conflicts the United States engages. The United States generally reserved the use of force to defend vital national interests, but the post-Cold War world changed that calculus. After the fall of the Soviet Union, the United States sought to promote its values throughout the world using military power and the AVF, in part, enabled this use of military power.

The United States in the post-Co**ld War world found itself as the world's lone superpower and** used that position to advance its values and principles instead of adhering to a strict defense of its vital national interests.[47] It became difficult for a president to justify inaction when people were **suffering throughout the world, and America's "**possession of matchless military capabilities not only endowed the United States with the ability to right wrongs and succor the afflicted, it also imposed an obligation to do just that."[48] President Clinton sent the U.S. military to solve conflicts in Somalia (though he did inherit this particular mission from his predecessor), Haiti, Bosnia, and Kosovo—conflicts of no strategic vital interest to the United States—and he did so unimpeded by the fact that he himself had avoided military service. While President Clinton weathered some criticism from the opposition party due to his lack of military service, he was enabled by the fact that the military of which he was the Commander in Chief was filled with men and woman who volunteered to be there. They were not forced into military service to fight a war as had as had been the case for many with respect to Vietnam. **They had essentially accepted the "King's Schilling" and as such would do the "King's bidding."** [49]

President Clinton's successor, George W. Bush, also benefited from the AVF. After the terror attacks of September 11, 2001, President Bush embarked on military campaigns in Afghanistan (2001) and Iraq (2003) ostensibly for reasons vital to U.S. national interests. Though he had served in the Air National Guard during the Vietnam War, he was criticized for avoiding service in Vietnam. But, again, the military he sent into Afghanistan and Iraq was composed of volunteers who chose to serve. As the wars dragged on, he neither raised taxes nor instituted conscription, thereby keeping **the vast majority of Americans from feeling the wars' effects.** President Bush won re-election in 2004, and the Republicans lost seats in the 2006 mid-terms due to public dissatisfaction with the war in Iraq. Republican senators did well in states and counties left relatively unaffected by casualties in Iraq, however.[50] Public sentiment toward the conflict in Iraq enabled President Bush to continue

---

[46] **Jeffrey Goldberg, "The Obama Doctrine,"** *The Atlantic Monthly* 317, no. 3 (April 2016): 70-90.

[47] Mandelbaum, *Mission Failure: America and the World in the Post-Cold War Era*, 368. See also Arnold A. Offner, "Liberation or Dominance? The Ideology of U.S. National Security Policy," in *The Long War: A New History of U.S. National Security Policy Since World War II*, ed. by Andrew J. Bacevich (New York: Columbia University Press, 2007), 2, 17, 35.

[48] Bacevich, *America's War for the Greater Middle East: A Military History*, 143.

[49] **Robert L. Goldich, "American Military Culture: Culture from Colony to Empire," in** *The Modern American Military*, ed. by David M. Kennedy (Oxford: Oxford University Press, 2013), 89.

[50] Douglas L. Kriner and Francis X. Shen, "Iraq Casualties and the 2006 Senate Elections," *Legislative Studies Quarterly* 32, no. 4 (November 2007): 508.

prosecuting that war effort—albeit after changing his strategy, operational approach, and leadership in both the Pentagon (civilian) and Iraq (military).

During the Obama presidency, the United States maintained forces in Afghanistan without much public pressure to withdraw those forces or demand campaign progress. As the president who fulfilled his campaign promise to withdraw U.S. troops from Iraq in 2012, he once again deployed forces (though in significantly fewer numbers, especially with regard to ground troops) to the region to fight ISIS in 2014. That conflict continues. Utilizing deficit spending without raising taxes, coupled with a volunteer military force, keeps the American public at bay and enables campaigns such as these to proceed without much national debate. As stated by French international relations scholar **Etienne de Durand, "Mobilizing the population generally comes with a heavy price tag attached to it; the nonnegotiable need to show quick results."**[51]

Conclusion

The United States' AVF enables the use of force by America's political leaders. The AVF is a powerful instrument, grounded in historic traditions and rooted in traditional liberal thought and philosophy concerning the relationship between the government and the governed in the defense of the nation. **Today's scholar**s who warn the AFV erodes the concept of civic duty for the defense of the **nation seem to have a love affair with the false notion that today's AVF is an aberration and** incompatible with the ideals of republican democracy; and that the AVF removes the American public from the national debate on the use of force simply because an overwhelming majority of **Americans do not choose to serve in their nation's armed forces.** While the AVF enables presidents to use military force more freely, they must do so with recognition that they cannot use it with total disregard for American public opinion or without consideration for how its use will affect the AVF overall.

The American public still retains an interest in how the AVF is used and has shown the ability to hold elected officials responsible. Americans place tremendous pride and trust in their armed forces and have immense respect for those who freely choose to serve in the military, especially in times of conflict. When they perceive that their military is being used in ways counter to the national values and interests, Americans tend to hold their politicians responsible. And, for their part, the political leaders acknowledge they have considerable leeway with regard to the use of military force. This leeway is not a blank check, however, and American political leaders must answer to American voters every election cycle.

Maintaining the AVF also requires willing volunteers. Men and women join the armed forces for any number of reasons, but they do so with the understanding that their lives will not be wasted in **military adventures that do not protect the nation's vital interests.** Americans who volunteer for military service essentially write a check to their government, payable with their lives, but with the expectation that they will not be cashed or frittered away on misadventures.[52] **America's political** leaders must keep this moral obligation in the forefront if they are to continue relying on volunteerism as the source of manpower for the U.S. military.

---

[51] Octavian Manea, "Reflections on the French School of Counter-Rebellion: An Interview with Etienne de Durand," *Small Wars Journal*, March 3, 2011. Quoted in Robert L. Goldich, "American Military Culture: Culture from Colony to Empire," 89.

[52] James Kurth, "Variations on the American Way of War," in *The Long War: A New History of U.S. National Security Policy Since World War II*, ed. by Andrew J. Bacevich (New York: Columbia University Press, 2007), 85.

Carl von **Clausewitz famously wrote that "war is an extension of politics."**[53] The use of force is a legitimate instrument of foreign policy, but should generally be used when diplomacy and other instruments of national power have failed. The United States will continue to employ its military force in the defense of the liberal international order because it cannot continue to thrive in a world hostile to its interests or values.[54] **America's political and military leaders must understand, therefore, that America's AVF** should not be an instrument of first resort simply because the American public writ large does not overwhelmingly contribute manpower to the military. If these **leaders desire to retain the AVF as America's military manpower system of choice, they will nee**d to rely on a steady stream of willing recruits to populate the force. That stream will dwindle to a trickle if the American public does not believe the lives of their servicemen and women are used in ways vital to the nation. **For this reason, America's l**eaders will always need the support of the American population before using military force.[55]

The United States is the world's preeminent military power. The foundation of this military power is the relatively few men and women who, with the overwhelming support and admiration of the American public, choose to serve. While it is reasonable that the American public would acquiesce to a draft to defend their country against an actual existential threat, contemporary policy seeks to keep threats well outside **the nation's borders such that the republic's survival remains secure. Historian T.R. Fehrenbach best described the importance of America's volunteer military when he** states:

> However repugnant the idea is to liberal societies, the man who will willingly defend the free world in the fringe areas is not the responsible citizen-soldier. The man who will go where his colors go, without asking, who will fight a phantom foe in jungle and mountain range, without counting, and who will suffer and die in the midst of incredible hardship, without complaint, is still what he always has been, from Imperial Rome to sceptered Britain to democratic America. He is the stuff of which legions are made.[56]

Volunteers, therefore, are both required and best suited to guard the posts at the fringes while preserving the liberal international order. **Therein lies the AVF's necessity and true value to the American people.**

---

[53] Carl von Clausewitz, *On War*, trans. and ed. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984).

[54] Eliot A. Cohen, *The Big Stick: The Limits of Soft Power and the Necessity of Military Force* (New York: Basic Books, 2016), 25.

[55] Burk, "The Changing Moral Contract for Military Service," 443.

[56] T.R. Fehrenbach, *This Kind of War: Korea, a Study in Unpreparedness* (New York: MacMillan, 1963), 658.

The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

SSI STRATEGIC STUDIES INSTITUTE	The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.
CSL CENTER for STRATEGIC LEADERSHIP U.S. ARMY WAR COLLEGE	The Center for Strategic Leadership contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.
PKSOI	The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.
SCHOOL OF STRATEGIC LANDPOWER U.S. Army War College	The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.
UNITED STATES ARMY HERITAGE AND EDUCATION CENTER	The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

THE
UNITED STATES
ARMY WAR COLLEGE

STRENGTH *and* WISDOM

U.S.ARMY