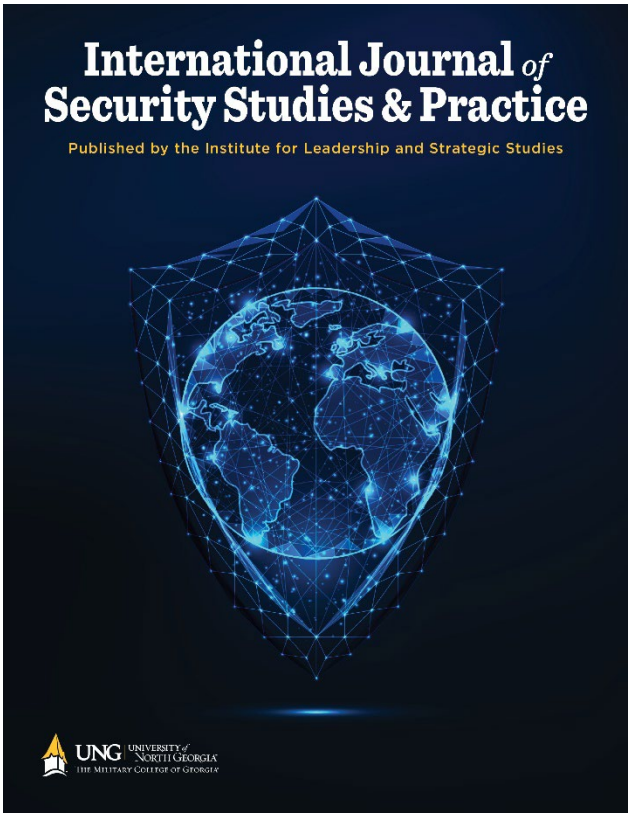
International Journal of Security Studies & Practice

Volume 2 | Issue 1

2022

Cyber (In)Security Within Contested Deployment

José de Arimatéia da Cruz
jose.a.dacruz.civ@army.mil



Cyber (In)Security Within Contested Deployment

José de Arimatéia da Cruz

jose.a.dacruz.civ@army.mil

José de Arimatéia da Cruz is a Professor at Georgia Southern University and Visiting Research Professor at the U.S. Army War College Center for Strategic Leadership Homeland Defense and Security Issues, Carlisle, PA. The views expressed herein are the author's own and in no way reflect the official position of the United States Government, Department of Defense, or the U.S. Army.

Author Note

The author has no known conflict of interest to disclose. Correspondence concerning this article should be addressed to José de Arimatéia da Cruz. Email: jose.a.dacruz.civ@army.mil

Abstract

The post-Cold War international system of the 21st century has not led to the "end of history," as argued by Francis Fukuyama in his seminal book *The End of History and the Last Man (1992).* Instead, the international system has become more complex with a revival of great power competition: a competition today that is not only kinetic but also occurs in cyberspace. Today's cyber-attacks against the U.S.'s critical infrastructure could have devastating consequences never seen before in the history of humanity. The enemy's ability to launch a cyber-attack against the U.S.'s critical infrastructure represents a significant security threat for the U.S. deployment of force to future operational theaters. This article examines who are the enemies within contested deployment; what are the enemies' objectives; what are the implications for the homeland; and finally, recommends what actions the U.S. could take to protect the homeland.

Cyber (In)Security Within Contested Deployment

"*The supreme art of war is to subdue the enemy without fighting.*"
- Sun Tzu's *The Art of War*

The post-Cold War international system of the 21st century has not led to the "end of history," as argued by Francis Fukuyama in his seminal book *The End of History and the Last Man* (1992). Instead, the international system has become more complex with a revival of great power competition. Today's competition for power is not only kinetic but also occurs in cyberspace. Cyber-attacks against a nation's critical infrastructure could have devastating consequences never seen before in the history of humanity. The international system of the 21st century has led not to the "end of history but rather to the "end of geography," where geographic boundaries have become porous, namely, through the cyber effect. Our enemies' ability to launch a cyber-attack against the U.S.'s critical infrastructure represents a significant security threat for the U.S. deployment of force projection to future operational theaters.

In fact, as former Secretary of Defense James Mattis succinctly pointed out, an enemy attack against the U.S.'s critical infrastructure must be expected and anticipated. He argued in his *Summary of the 2018 National Defense Strategy of the United States* that

> It is now undeniable that the homeland is no longer a sanctuary. America is a target of terrorists seeking to attack our citizens, malicious cyber activity against personal, commercial, or government infrastructure, or political and information subversion. New threats to commercial and military use of space are emerging, while increasing digital connectivity of all aspects of life, business, government, and military creates significant vulnerabilities. During the conflict, attacks against our critical defense, government, and economic infrastructure must be anticipated. (Mattis, 2018)

One of the consequences for the nation-state in an interconnected global society is that its critical infrastructures (CIs) are composed of public and private institutions of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials sectors, all of which are vulnerable to cyber-attacks. Audrey Kurth Cronin pointed out, "insurgents and terrorist groups have effectively used the Internet to support their operations for at least a decade. The tools of the global information age have helped them with administrative tasks, coordination of operations, recruitment of potential members, and communications among adherents" (2013). Using cyber weapons to carry on an attack against the U.S.'s critical infrastructure while pursuing plausible deniability is one of the hallmarks of a cyber-attack. Cyber-attacks against the U.S. will become ever more prevalent within a contest deployment.

The New Environment Milieu: Cybersecurity, Cyberattacks, and More…

At his confirmation hearing, former Secretary of State John Kerry called cyber-attacks against the U.S.'s critical infrastructure a "twenty-first-century nuclear weapons equivalent" (Negroponte & Palmisano, 2013, p. 23). In the cyber world of the twenty-first century, the Internet is the realization of the classic international relations theory of an anarchic, leaderless world (Schmidt and Cohen, 2013). The importance of all the cyber tools available, known and unknown to friends and foes of the United States, is a force multiplier in the eventuality of a conflict between near-peer competitors or challengers to the U.S.'s hegemony in the aftermath of the implosion of the Soviet Union in 1991.

Competition and potential conflict between nation-states remain critical national security threats to homeland defense. The recent Annual Threat Assessment of the U.S. Intelligence Community released by the Office of the Director of National Intelligence released on February

2022 highlighted that "diffusion of power is leading to reassess their [the U.S. and its allies] place and capabilities in an increasingly multipolar world" (Annual Threat Assessment, 2022, p. 4). China, Moscow, Iran, and North Korea have demonstrated "the capabilities and intent to advance their interest at the expense of the United States and its allies" (Annual Threat Assessment 2022, p. 4). According to the Annual Threat Assessment, China "presents the broadest, most active, and persistent cyber espionage threat to the U.S. Government and private sector networks" (p. 8). Furthermore, given China's increasing cyber weaponization of its military capabilities, Beijing's "pursuits and export of related technologies increase the threats of attacks against the U.S. homeland, suppression of U.S. web content that Beijing views as threatening to its control, and the expansion of technology of technology-driven authoritarianism globally" (Annual Threat Assessment, p. 8). In the Annual Threat Assessment, China is "accelerating the development of critical capabilities it believes the People's Liberation Army (PLA) needs to confront the United States in a large-scale, sustained conflict (p. 7).

The Annual Threat Assessment emphasizes that Russia is another near-peer competitor to the United States. It will remain an influential power and a formidable challenge to the United States amidst the challenges and changes in the geopolitical landscape during the next decade (Annual Threat Assessment, 2022). The implosion of the Soviet Union on the eve of December 25, 1991, has been heralded by pundits and Sovietologists as an unprecedented event in world history. No one expected the mighty Union of Soviet Socialist Republics (USSR) to end as uneventfully as it did. The rise of Vladimir Putin to power in Russia, however, has set in motion a new attempt by Russia to find its proper place in the world within what Putin calls an emerging polycentric world order (da Cruz, 2015). Russia has become a cyber menace that the United States and its allies cannot ignore. The Annual Threat Assessment projects that Russia "will remain a top

cyber threat as it refines and employs its espionage, influence, and attack capabilities" (p. 12). Russia and its cyber proxies are actively engaged worldwide to undermine and attack any entities, governments, or the private sectors, that it considers hostile to undermine its "interests or threaten the stability of the Russian Government" (Annual Threat Assessment 2022, p. 12). Examples of Russia using its cyber capabilities to undermine its adversaries include cyber-attacks against Estonia and the Republic of Georgia. The Russian Government and its cyber proxies were also heavily involved in the U.S.'s 2016 presidential elections (Kim, 2020). Russia is also heavily investing in its electronic warfare capabilities to "counter Western on-orbit assets" (Annual Threat Assessment 2022, p. 13). Russia's electronic warfare weapons will disable and disrupt an adversary's "command, control, communication, computer, intelligence, surveillance, and reconnaissance (C4ISR) capabilities" (Annual Threat Assessment 2022, p. 13).

In the 2002 State of the Union address President Bush delivered to a nationally televised joint session of Congress, the President referred to Iraq, Iran, and North Korea as an "axis of evil." David Frum, one of the speech writers for President Bush, noted:

> States like these, and their terrorist allies, constitute an axis of evil, arming to threaten the world's peace. These regimes pose a grave and growing danger by seeking weapons of mass destruction. They could provide these arms to terrorists, giving them the means to match their hatred. They could attack our allies or attempt to blackmail the United States. In any of these cases, the price of indifference would be catastrophic. (2022)

While some political commentators and pundits have referred to Iran and North Korea as the "axis of evil," others prefer to use the term "axis of annoyance" (Arnson, Esfandiari & Stubits, n.d., p. 18). Regardless of the terminology used to describe the Islamic Republic of Iran and North Korea,

one constant is the fact that they are both a threat to the national security and homeland defense of the United States. Iran's growing expertise and willingness to conduct aggressive cyber operations, according to the Annual Threat Assessment 2022, make it a significant threat to the security of the U.S. and allied networks and data. Iran does not want a direct symmetric conflict with the U.S. Armed Forces. It would be a disaster for Iran and its ayatollahs in power. However, the Islamic Republic of Iran will use its cyber capabilities and malign influence in the region to undermine the interests of the United States in the Middle East. Furthermore, Iran's unconventional warfare operations and network of militant partners and proxies enable Tehran to advance its interests in the greater Middle East and maintain its strategic depth, according to the Annual Threat Assessment.

North Korea, according to the German Council on Foreign Relations, "is among the least wired countries worldwide. Yet, an increasing number of cyber activities are attributed to the regime in Pyongyang – and these activities have shown growing sophistication and success over the last few years. Its cyber operations will continue to increase as they fulfill at least three strategic purposes and exhibit a favorable cost-benefit ratio for the North Korean regime" (Suh, 2022, p. 1). As the 2022 Annual Threat Assessment points out, "North Korea's cyber program poses sophisticated and agile espionage, cybercrime, and attack threat" (p. 17). The Annual Threat Assessment argues that "Pyongyang is well positioned to conduct surprise cyber-attacks given its stealth and history of bold action" (Annual Threat Assessment, p. 17). There are several examples of such bold action by North Korea. One instance occurred in 2014 when North Korean hackers associated with the infamous Reconnaissance General Bureau's Bureau 121 hacked into Sony Pictures computer systems in retaliation for producing *The Interview*, a movie featuring James Franco and Seth Rogen, a fictional story of a CIA plot to kill the Hermit Kingdom's beloved leader,

King Jung-un. Another bold action by the North Korean regime occurred in 2016 when North Korean hackers planned a $1 billion raid on Bangladesh's national bank (Banka, 2021).

In addition to our traditional near-peer competitors challenging U.S. supremacy, the United States Armed Forces must also deal with and address other issues which are part of the new cyber environment. For example, terrorist organizations utilize the Internet as an essential part of their information operations (IOs) and offensive strategic objectives. Future conflicts in the twenty-first century will extend into cyberspace from the physical domain. Former President Obama, in his "International Strategy for Cyberspace," acknowledged that "cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace" (International Strategy for Cyberspace, 2011, p. 4).

Transnational Criminal Organizations (TCOs) also pose a direct threat to the United States and its allies "through human trafficking, the production and trafficking of lethal illicit drugs, cyber-crime, and financial crimes and money laundering schemes eroding the integrity of the international financial system" (Annual Threat Assessment, 2022, p. 23). According to the Federal Bureau of Investigation Internet Crime Report (2021) produced by the Internet Crime Complaint Center (IC3), in 2021, IC3 received 847,376 cyber complaints and reported a net loss of US$ 6.9 billion. The top five crimes in 2021 were: extortion (39,360 cases), identity theft (51,629), personal data breach (51,829 cases), Non-payment/Non-Delivery (82,478 cases), and Phishing/Vishing/Smishing/Pharming (323,972 cases).

Another critical issue in this new battle environment of the 21st Century is deepfake and how it contributes to a new disinformation war in the coming age of post-truth politics (Chesney & Citron, 2019). Deepfakes are highly realistic video montages in which a video is manipulated to resemble one's actions in terms of image and voicing. Deepfakes use a form of artificial

intelligence called deep learning to make images of fake events, hence the name deepfake (Sample, 2020). Deepfakes and the proliferation of fake news in the online environment have only been possible with the exponential growth in the digital influence of mercenaries. The digital influence of mercenaries' rise is also due to the simple economic forces of supply and demand (Forest, 2022). Digital influence mercenaries claim "their services only focus on criminals and "terrorists; Meta's months-long investigation concluded that targeting is indiscriminate and includes journalists, dissidents, critics of authoritarian governments, families of opposition, and human rights activists (Aljazeera, 2021). Digital influence mercenaries are called trolls and virtual mercenaries. Their skill sets are available on the gray market to the highest bidder, be it a nation-state, non-state actor, terrorist organization, or private individual.

Contested Deployment

The "shining city upon the hill" is no longer a safe haven. The traditional realist geopolitical view that two oceans, the Pacific and the Atlantic, and two benevolent neighbors, Canada and Mexico, isolate the United States from the rest of the world is no longer realistic. The "end of history" has not made the world more secure; instead, it has led to the "end of geography," where boundaries have become more porous than ever, considering the process of globalization and advancement in technology. Near-peer friends or foes will not wait for the United States to bring the war to them in its own time, place, and resolve. Instead, the enemies will bring the battle to the United States before the conflict even starts by utilizing all means necessary, including, but not limited to, cyber-attacks, Distributed-Denial-of-Service (DDoS), hacking, Denial-of-Service (DoS), and other nefarious activities. As Bert Tussing, director of Homeland Defense and Security Studies at the U.S. Army War College, argues, "preparations for battle begin in the homeland. The home front will be part of the next major battlefield, and the price of poor preparation will be paid

by soldiers and civilians alike. To ensure US forces are organized, trained, equipped, and postured, we must develop battle concepts that consider the domestic battlefield. We cannot win 'over there' if we lose 'over here'" (Tussing, Powell & Leitzel, 2022, p. 2). In other words, "war is changing, the threat is changing, and the United States and its Army need to adapt to these changes" (Tussing, Powell & Leitzel, p. 9).

Contested deployment is a concept that emerged from an integrated research project conducted by Bert Tussing, John Eric Power, and Benjamin C. Leitzel at the Center for Strategic Leadership at the U.S. Army War College. Tussing, Power, and Leitzel defined contested deployment as "deployment operations faced with incidental, inadvertent, or deliberate obstruction, resulting in a prohibition of, or significant delay in, the relocation of forces and material to desired operational areas" (p. 1). In other words, in the battles of the 21st century, the most powerful and capable armies will not necessarily win the conflict. Therefore, the U.S. Army must adapt and adjust to this changing nature of conflicts. The Army of the 21st century must be nimble. The future enemies will not pursue a direct conflict with the United States and its Army. Instead, they will operate just below the "gray zone," that area of conflict in which adversaries can carry out their nefarious activities while asserting plausible deniability. Another characteristic of disputes within a contest deployment is that the U.S. Government and its Army will not be able to go alone. Conflict in contested deployment will require a whole-of-government approach involving all agencies of the federal government and the private sector. Especially since the private sector controls roughly 85% of the critical infrastructure which the U.S. Government and its Army rely upon during wartime.

Implications

The Department of Defense designated cyberspace a new domain of warfare in 2011. This elevation in strategic importance makes cyberspace comparable to land, sea, air, or outer space as a new battle frontier. The U.S. government and the Army recognize cyberspace as a potential future battleground. Cybersecurity will be a significant concern during contested deployment. Former Defense Secretary Leon Panetta explicitly stated that "cyberspace is the new frontier, full of possibilities to advance security and prosperity in the 21st century. And yet, with these possibilities, also come new perils and new dangers" (Panetta, 2012). The former Chairman of the Joint Chiefs of Staff, Army General Martin E. Dempsey, stated that "the Department of Defense is adding a new mission: defending the nation, when asked, from attacks of significant consequence—those that threaten life, limb, and the country's core critical infrastructure" (Roulo, 2013).

Another vital implication considering contested deployment is protecting or lacking the U.S.'s defense industry. Travis Howard argues that the biggest threat to U.S. national security is not a zero-day exploit or fancy-coded malware but rather "the biggest, long-term threat to national security is the rampant exfiltration of America's technological advantages from the defense industrial base" (Howard, 2020, p. 1).

Recommendations

Four traditional instruments of national power–diplomacy, information, military, and economic–are referred to by the abbreviation DIME. While the DIME construct has been used widely for many years, the post-Cold War era has introduced additional elements that do not fit the traditional approach. These include law enforcement, intelligence, and financial entities. Accordingly, the DIME has been modified to incorporate these other elements of national power,

resulting in the DIMEFIL, comprised of the following instruments of emphasis: diplomacy, information, military, economic, financial, intelligence, and law enforcement.

The mirror concept to the DIMEFIL construct, especially as it applies to the U.S. Government and the Army, is known as the **PMESII. The PMESII** provides a systemic way to identify the entities against which a nation may employ as the instruments of its national projection and national power. PMESII comprises **P**olitical, **M**ilitary, **E**conomic, **S**ocial, **I**nfrastructure, and **I**nformation elements, encompassing all the aspects an entity could possess to achieve national policy objectives. The United States, especially its Army and allies, must take a whole-of-government approach when addressing cyber (in)security in the post-Cold War international system. As the Cyberspace Solarium Commission (2020) reported, "the United States lacks a clear, comprehensive, publicly declared doctrine that incorporates all of the instruments of power to address less-than-catastrophic attacks on public and private networks in cyberspace" (p. 14). This paper offers the following recommendations. This is not an exhaustive recommendations list.

First, the US Government must build a public-private partnership in which the private sector sees the U.S. Government as a dependable partner. The private sector's reluctance to share cyber-attack data with the U.S. Government results from unclear directives and how the data may be used or with whom the U.S. Government may share it. Companies protecting reputation, market values, and shared holders are reluctant to partner with the U.S. Government. Under a contested deployment, this partnership between the U.S. Government and the privates recognizing each other as valuable and coequal will be more critical than ever since the enemies will challenge the homeland in the next major U.S. war. If such a partnership is not advanced, "public and private sector responses are left uncoordinated, and the nation's critical infrastructure is left unprotected and vulnerable to adversaries who can, and will, exploit this opportunity" (Cyberspace Solarium

Commission, 2020, p. 17).

Second, the U.S. Government and its Army must continue emphasizing zero trust architecture and talent acquisition. A zero-trust architecture approach to cybersecurity is based on the principle of "always verify" (Cybersecurity Infrastructure & Security Agency, n.d.). Zero-trust is the modern-day principle of the Reagan doctrine of "trust but verify." As Steven Grossman has pointed out, President Ronald Reagan taught us to "trust but verify," meaning trust is great, but blind faith is dangerous (Grossman, 2017). A zero-trust approach assumes that the only computer which is not subjected to an attack is one that is turned on. As President Joe Biden's Executive Order 14028 of May 12, 2021, points out, the zero-trust security model "eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses" (Exec. Order No. 14028, 2021). In other words, the zero-trust approach "explicitly verifies every request for access, regardless of where it originates or what resources it accesses" (Cybersecurity Infrastructure & Security Agency, n.d.).

According to Cybercrime Magazine, **"**over an eight-year period tracked by Cybersecurity Ventures, the number of unfilled cybersecurity jobs grew by 350 percent, from one million positions in 2013 to 3.5 million in 2021" (Morgan, 2021). The third recommendation is talent acquisition. Talent acquisition will be a challenge to the U.S. Government and its Army. Talent acquisition has not gone unnoticed by the U.S. Government and its Army. Dr. Raj Iyer, Army Chief Information Office (CIO) at the United States Army Europe and Africa 2022 Cybersecurity Summit, held on July 29, highlighted talent acquisition's importance to the Army's future combat capabilities, power projection, and cyber workforce. As Dr. Iyer pointed out, **"**finding the right people is one of his biggest challenges as Army CIO. He emphasized the importance of filling the

cyber talent gap and that the Army plans to address this perennial challenge by rolling out the Cyber Excepted Service, a new talent model for the civilian cyber workforce, this year. The service will take advantage of every available tool to recruit and retain the cyber workforce" (Vega, 2022). Unfortunately, one of the tools not available to the Army is the high compensation package provided by the private sector to cybersecurity professionals. For example, "positions including cybersecurity analyst, information security analyst, and penetration tester, and annual median salaries ranging from $75,000 to more than $100,000" (Morgan, 2021). Dr. Iyer recognizes the talent acquisition dilemma facing the U.S. Government and its Army when he stated, "I always tell people if you're going to come work for the Army in this cyberspace, you're not doing it for the monetary benefits," he said. "You are doing it because you now have a serious role in protecting the nation, just like any other cyber warrior, whether you're wearing the uniform or not" (Vega. 2022).

The U.S. Government and its Army must continue to implement and follow the guidelines of the Cyberspace Solarium Commission by implementing its layered cyber deterrence. This cybersecurity strategy emphasizes a three-layered approach to achieve its end goal. First, shape behavior. According to the Cyberspace Solarium Commission, "In the first layer, the strategy calls for shaping responsible behavior and encouraging restraint in cyberspace by strengthening norms and non-military instruments. Effective norms will not emerge without American leadership. For this reason, the United States needs to build a coalition of partners and allies to secure its shared interests and values in cyberspace" (U.S. Cyberspace Solarium Commission, 2020, p. 3). The second layer is to deny benefits to those attacking the U.S.'s cybersecurity critical infrastructure. "In the second layer, the strategy calls for denying benefits to adversaries by promoting national resilience, reshaping the cyber ecosystem, and advancing the government's relationship with the

private sector to establish an enhanced level of common situational awareness and collaboration. The United States needs a whole-of-nation approach to secure its interests and institutions in cyberspace" (U.S. Cyberspace Solarium Commission, p. 4). The third layer of the layered defense deterrence strategic approach to cybersecurity emphasizes the costs to those attacking the U.S. cybersecurity by using all the instruments of state power under the PMESII (**P**olitical, **M**ilitary, **E**conomic, **S**ocial, **I**nfrastructure, and **I**nformation). According to the Cyberspace Solarium Commission,

> In the final layer, the strategy outlines how to impose costs to deter future malicious behavior and reduce ongoing adversary activities short of armed conflict through the employment of all instruments of power in defense of cyberspace, including systemically important critical infrastructure. A key, but not the only, element of cost imposition is the military instrument of power. Therefore, the United States must maintain the capacity, resilience, and readiness to employ cyber and non-cyber capabilities across the spectrum of engagement, from competition to crisis and conflict. The United States needs ready and resilient capabilities to thwart and respond to adversary action. (U.S. Cyberspace Solarium Commission, p. 6)

Two distinct factors enhance the U.S. Government's layered cyber deterrence. First, layered cyber deterrence prioritizes deterrence by denial. To accomplish that goal, the U.S. Government and its Army must increase "the defense and security of cyberspace through resilience and public- and private-sector collaboration. Reducing the vulnerabilities adversaries can target denies them opportunities to attack American interests through cyberspace" (U.S. Cyberspace Solarium Commission, p. 2). Resilience within the context of layered cyber deterrence means "the capacity to withstand and quickly recover from attacks that could cause harm or coerce, deter, restrain, or

otherwise shape U.S. behavior" (U.S. Cyberspace Solarium Commission, p. 4).

Finally, as the U.S. Army continues developing and enhancing its multidomain operations concept, cybersecurity will be an integral part of these new multidomain operations. Jen Judson, a journalist covering land warfare for Defense News, said "The doctrine will address great power competition and potential conflict with near-peer adversaries across air, land, sea, space, and cyberspace" (2022, p. 1). Army Space, Cyber, and Special Operations Command recently formed the "triad" to strike anywhere, anytime. According to Lieutenant General Jon Braga, commander of the United States Army Special Operations Command, "Information operations are critical, influence operations are extremely important, contributing to integrated deterrence is extremely important," but should operations move into conflict, the triad would have a different role to play, possibly "a combination of non-lethal effects like information operations, then perhaps a more kinetic [option], denying a capability or affecting a certain capability of an adversary — that would be a different flavor of approach" (Judson, 2022, p. 1).

Conclusion

Within a contested deployment, the enemies will not wait until the U.S. Government and its Army brings them the war. The homeland will be a target in the future by near-peer enemies. No nation-state will go head-to-head against the United States and its Army in a kinetic conflict. The near-peer adversaries will use a combination of irregular warfare enhanced by cyber disruption and disabling adversary command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR). Multiple trends are shaping the technology landscape of the following decades; therefore, the United States and its Army must be prepared for the nature of new conflicts in the 21st century. The United States and its Army must be alerted and resolved to protect, deflect, and counterattack enemies across air, land, sea, space, and cyberspace. The U.S.

Government and its Army must be forever vigilant in this new cyber ecosystem in which misinformation, disinformation, and malinformation (so-called MDM) have become an integral part of any conflict. Cyber operations within this new multidomain operations concept will afford near-peer adversaries, including non-state actors, with "instruments of coercion, sabotage, espionage, and extortion optimized for the 21st century" (U.S. Cyberspace Solarium Commission, 2020, p. 8). Sun Tzu said in the Art of War, "subjugating the enemy's army without fighting is the true pinnacle of excellence" (Sawyer, 1994, p. 177) The United States and its Army must take a leadership role in this new battlefield of the 21st century or ignore it at its own peril.

References

Aljazeera. (2021, December 17). *Meta bans 'cyber-mercenaries' that targeted 50,000 people.* https://www.aljazeera.com/news/2021/12/17/meta-bans-cyber-mercenaries-spying-on-journalists-activists

Arnson, C., Esfandiari, H., & Stubits, A. (n.d.). *Iran in Latin America: Threat or axis of annoyance?* (Report no. 23). Woodrow Wilson International Center Reports on the Americas. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/Iran_in_LA.pdf

Banka, N. (2021, June 30). *Explained: The story of how North Korean hackers stole $81 million from Bangladesh Bank*. The Indian Express. https://indianexpress.com/article/explained/bangladesh-bank-robbery-north-korea-lazarus-heist-7375441/

Chesney, R., & Citron, D. (2019, January/February). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. *Foreign Affairs. 98*(1), 147-155. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war

Cybersecurity Infrastructure & Security Agency. (n.d.). *Election Infrastructure Insider Threat Mitigation Guide.* https://www.cisa.gov/sites/default/files/publications/election_insider_threat_mitigation_guide_508_0.pdf

Cronin, A. K. (2013, Winter/Spring). How global communications are changing the character of war. *The Whitehead Journal of Diplomacy and International Relations,* 25-39. https://ciaotest.cc.columbia.edu/journals/shjdir/v14i1/f_0028740_23334.pdf

da Cruz, Jose de Arimateia. (2015). Strategic Insights: From Ideology to Geopolitics: Russian Interests in Latin America. Retrieved August 14, 2022. Available at https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1486&context=articles_editorials

Exec. Order No. 14028, 3 C.F.R. (2021). https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

Federal Bureau of Investigation. (2021). Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Forest, J. F. (2022). *Digital influence mercenaries: Profits and power through information warfare.* Naval Institute Press.

Frum, D. (2022, January 29). The enduring lessons of the 'axis of evil' speech. *The Atlantic*. https://www.theatlantic.com/ideas/archive/2022/01/axis-of-evil-speech-frum-bush/621397/

Fukuyama, F. (1992). *The end of history and the last man.* Free Press.

Grossman, S. (2017, December 20). **Behavioral analytics enables verification that users are doing the right thing, and promotes transparency. *Security Week.*** https://www.securityweek.com/words-president-ronald-reagan-trust-verify

Howard, T. (2020). *Protecting America's defense industrial advantages in cyberspace.* Institute for Critical Infrastructure Technology (ICIT). https://img1.wsimg.com/blobby/go/cf7bb6e3-4c42-4952-a4a2-2dc45c48c25b/downloads/ICIT-Member-Perspective-Essay-Travis-Howard-De.pdf?ver=1633110053994

The White House. (2011, May). *International strategy for cyberspace: Prosperity, security, and openness in a networked world.* https://apps.dtic.mil/sti/pdfs/ADA543951.pdf

Judson, J. (2022, March 23). Multidomain operations concept will become doctrine this summer. *Defense News.* https://www.defensenews.com/land/2022/03/23/multidomain-operations-concept-will-become-doctrine-this-summer/

Kim, Y. M. (2020, March 5). New evidence shows how Russia's election interference has gotten more brazen. *Brennan Center for Justice.* https://www.brennancenter.org/our-work/analysis-opinion/new-evidence-shows-how-russias-election-interference-has-gotten-more

Mattis, J. N. (2018). *Summary of the 2018 national defense strategy of the United States.* Department of Defense. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

Morgan, S. (2021). Cybersecurity jobs report: 3.5 million openings by 2025. *Cybercrimes Magazine.* https://cybersecurityventures.com/jobs/

Negroponte, J. D., & Palmisano, S. J. (2013, June). *Defending on open, global, secure, and resilient internet. (Report No. 70).* Council on Foreign Relations. https://www.cfr.org/report/defending-open-global-secure-and-resilient-internet

Office of the Director of National Intelligence. (2022, February 7). *Annual Threat Assessment of the U.S. Intelligence Community*. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2022-Unclassified-Report.pdf

Panetta, L. (2012, October 12). Remarks by Secretary Panetta on cybersecurity to the business executives for national security, New York City. https://content.govdelivery.com/accounts/USDOD/bulletins/571813

Roulo, C. (2013, June 28). DOD must stay ahead of the cyber threat, Dempsy says. *Patch.* https://patch.com/north-carolina/fortbragg/gen-dempsey-dod-must-stay-ahead-of-cyber-threat

Sample, I. (2020, January 13). What are deepfakes—and how can you stop them? *The Guardian.* https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them

Sawyer, R. D. (1994). *Sun-Tzu: The art of war.* Westview Press Inc. (Original work published between 425 and 221 B.C.E.)

Schmidt, E., & Cohen, J. (2012). *The new digital age: Reshaping the future of people, nations, and business.* Alfred A. Knopf.

Suh, E. (2022, January 7). North Korea's cyber capability and strategy. *German Council on International Relations.* https://dgap.org/en/research/publications/north-koreas-cyber-capabilities-and-strategy-0

Tussing, B. B., Powell, J. E., & Leitzel, B. C. (2022, April 26). *Contested deployment: Integrated research project* [Audio podcast]. Decisive Point. US Army War College Press. https://ssi.armywarcollege.edu/2022/podcast/mr-bert-b-tussing-dr-john-eric-powell-and-col-benjamin-c-leitzel-contested-deployment/

U.S. Cyberspace Solarium Commission (2020, March). https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

Vega, S. (2022, August 10). *Army CIO speaks at Army Europe and Africa 2022 cybersecurity summit.* Army Office of Chief Information Officer. *https://www.army.mil/article/259218/army_cio_speaks_at_army_europe_and_africa_2022_cybersecurity_summit*