VOLUME 9 ◆ NUMBER 3 FALL 2024

THE CYBER DEFENSE REVIEW

The Need for a Cyber Smoke Screen: A Tactical Action that Instantly Becomes Strategic in an All-Domain Operation

Dr. Dan G. Cox

The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield
Joshua Baughman

Blind Allegations of U.S. Cyber Hegemony Complements China's Influence Campaign to Weaken Global Confidence in the United States
Emilio Iasiello

GenAI in the 2024 Taiwan Presidential Election: Lessons for Democracies
Maj. Sarah Mobilio

Embracing Memory Safe APIs for C2 Systems
Capt. Brian Yarbrough and Maj. Phelan Guan

Forward Persistence in Great Power Cyber Competition: Military Assets in a Relative Power Erosion Framework
Dr. Thomas F. Lynch III

INTRODUCTION
Reimagining the Future

Editor-in-Chief,
Deborah S. Karagosian

ARMY CYBER INSTITUTE ◆ WEST POINT PRESS

The Cyber Defense Review

Fall Edition

THE CYBER DEFENSE REVIEW

A DYNAMIC MULTIDISCIPLINARY DIALOGUE

CONTACT
West Point Press
Taylor Hall, Building 600
West Point, NY 10996

SUBMISSIONS
The Cyber Defense Review
welcomes submissions at
TheCyberDefenseReview@westpoint.edu

WEBSITE
cyberdefensereview.army.mil

The Cyber Defense Review (ISSN 2474-2120) is published by the West Point Press. The views expressed in the journal are those of the authors and not the United States Military Academy, the Department of the Army, or any other agency of the U.S. Government. The mention of companies and/or products is for demonstrative purposes only and does not constitute endorsement by United States Military Academy, the Department of the Army, or any other agency of the U.S. Government.

This publication of the CDR was designed and produced by Gina Daschbach Marketing, LLC, under the management of FedWriters.
The CDR is printed by McDonald & Eudy Printers, Inc. ∞ Printed on Acid Free paper.

INTRODUCTION

PROFESSIONAL COMMENTARY

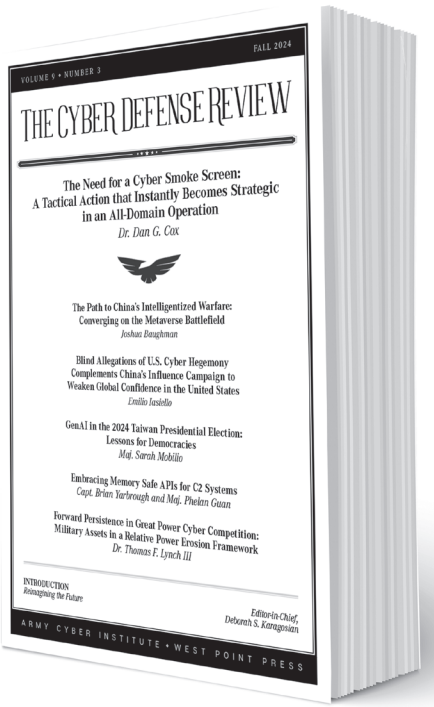
RESEARCH ARTICLES

The Cyber Defense Review

Introduction

Reimagining the Future

Deborah S. Karagosian



The Fall Edition of *The Cyber Defense Review* is largely influenced by the need for all of us to reimagine the future. How do we help create positions of relative advantage in competition while also preparing for future crisis and conflict? Our nation has recognized that the People's Republic of China (PRC) has studied how we conduct war and implemented approaches that, according to GEN Mark Milley, "pursue their strategic objectives while avoiding the deterrent tripwires upon which our national security posture is based." While we are "at war" in the cyber domain every day, the reality is we are a huge player in strategic competition. Reimagining the future includes making adjustments and preparing for crisis and conflict. As we study our adversaries and embark on new missions, technology continues to evolve, as do the ways people employ it.

Deborah S. Karagosian is the Editor-in-Chief of *The Cyber Defense Review* (CDR) at the United States Military Academy (USMA) at West Point, New York. In this capacity, she publishes the flagship cyber journal for the U.S. Army and Department of Defense. Before this assignment, she was an executive at two defense firms, entrepreneur, developer, consultant, and Soldier. She served the Army for 22 years with deployments to Asia, the Balkans, Africa, and the Middle East. She is a 1994 graduate of USMA and earned a M.S. in Computer Systems Engineering, an MBA in Strategic Management, and an MMAS from the School of Advanced Military Studies (SAMS).

Our cyber community is reimagining the future of warfare based on the lessons we learned, and continue to learn, in Nagorno-Karabakh, Gaza, Ukraine, and Israel. For good and bad, the innovative development of new technologies, applied in new ways in this battlespace will make it more lethal, reduce the ability to hide, and increase the tempo of war. The articles in this edition focus on visualizing the future operational environment, understanding our pacing threat, and leveraging lessons learned and research to improve our ability to compete and win.

This Fall Edition starts with Dr. Dan Cox of the School of Advanced Military Studies (SAMS) discussing "The Need for a Cyber Smoke Screen: A Tactical Action that Instantly Becomes Strategic in an All-Domain Operation." The proliferation of sensors across the battlefield is making our battle space increasingly transparent, necessitating cyber smoke screens to disable all sensors and devices in a region to successfully maneuver. While defensive in nature, a cyber smoke screen is an offensive cyber operation, suggesting that it may be time to integrate offensive and defensive cyber operations. Dr. Cox advocates for a cautious and mindful approach when military necessity calls for large-scale and prolonged disruption of internet services.

The intelligence community and our cyber mission forces will need a focused, sustained effort to understand the ever-changing terrain, both real-world and virtual, on and through which our Army will fight in the future. Preparing for information advantages will also require an understanding of the indigenous networks, peoples, and platforms where our Joint Force may be expected to compete or fight in the future. This edition contains three articles focused on understanding our pacing threat.

In his article, "The Path to China's Intelligentized Warfare: Converging on the Metaverse," Josh Baughman offers a unique perspective on how the PRC and the

People's Liberation Army (PLA) are leveraging emerging technologies in a new "intelligentized" era to create asymmetric advantages. In the PLA's "Meta-War," whoever can effectively integrate and connect the real world with virtual ones will have the "innovation high ground" to achieve the PRC's digital grand strategy and win future wars. His analysis provides timely and relevant insight into not only how the PLA thinks metaverse wars will be fought but also on how they envision they will be won.

The PRC strategically uses information to paint negative perceptions of U.S. actions within China and on the global stage. Everything in unclassified spaces, on the news, and in social media can be used by the Chinese Communist Party (CCP) to influence both their domestic population and international sentiment away from the U.S. and toward PRC goals. In "Blind Allegations of U.S. Cyber Hegemony Complements China's Influence Campaign to Weaken Global Confidence in the United States," Emilio Iasiello presents the cyber and geopolitical themes used by the PRC in Chinese and international news outlets and social media to label U.S. cyber activities as hegemonic, designed to exert influence and control the global internet, and to depict the U.S. as a "flawed democracy" that pervasively interferes in other state's affairs. Mr. Iasiello argues that PRC media campaigns may be aimed at influencing members of the United Nations to align with either a PRC or Russian preference for a government-led approach to internet governance to build "true power" by setting the standards and norms in the domain where such battles will be fought.

In his book *Next War: Reimagining How We Fight*, John Antal states artificial intelligence will change the speed at which we conduct war. But, if the PRC looks to achieve its national digital strategy without combat, how will it use technology during competition, and how can we counter it without raising the stakes? Major Sarah Mobilio discusses how the PRC used GenAI to influence Taiwan's 2024 national election and how the government of Taiwan responded in "GenAI in the 2024 Taiwan Presidential Election: Lessons for Democracies." While the PRC has increasingly used GenAI to craft subtle and increasingly undetectable influence campaigns, Taiwan's multi-faceted response, which included legislative actions, media literacy initiatives, and the development of its own GenAI tools, offers valuable insights for other countries facing similar challenges. Reimagining the future may include developing AI to counter the AI being used against us.

As our Army and Joint Force seek to gain positions of relative advantage in the information space, Captain Brian Yarbrough and Major Phelan Guan discuss the urgent need for "Embracing Memory-Safe APIs for C2 Systems." The information exchange enabled by Joint All-Domain Command and Control (JADC2) and many innovative initiatives throughout the force rely on the secure implementation of Application Program Interfaces (APIs). However, using inherently insecure languages creates strategic and tactical risks to DoD command and control, artificial intelligence, and legacy systems. Captain Yarbrough and Major Guan present these risks while providing recommendations for migrating to modern memory- and

type-safe programming languages and mitigating risks from other languages. We need to reimagine software development for our DoD systems and all public and private sector systems that rely extensively on APIs to communicate between systems and conduct business logic.

Similar to the risks Captain Yarbough and Major Guan address above, adversary targeting of a vulnerability is not limited to DoD networks. Attacks on critical national infrastructure are becoming a new normal in U.S. society. This era of Great Power Competition has led to changes in U.S. national strategies, and within DoD we are reimagining how to fight along the continuum of military operations. Dr. Tom Lynch of the National Defense University proposes the U.S. pursue a Relative Power Erosion framework that uses all elements of U.S. national power to create strategic cyber campaigns (and counter cyber campaigns) designed against PRC and Russian cyber organizations. He states that while USCYBERCOM's persistent engagement and hunt forward strategy appears effective in the near term, it is not sufficient for the longer term. Dr. Lynch suggests that the U.S. establish civilian interagency teams to operate as the military CMF teams operate today as they would be better suited to a whole-of-government approach for creating relative power gains and countering the efforts of U.S.'s great power rivals.

The technology and innovation inherent in our profession require the members of our community to learn constantly. We are always looking at vulnerabilities, the TTPs of hackers, and ways to employ new technologies to make our domain more secure and create new ways to access and impose our will on and through the networks of our adversaries. Reimagining the future requires our community to expand our thinking to understand more of the world around us and how our great power rivals are leveraging information, the electromagnetic spectrum, and cyberspace to build power. We hope the articles presented here increase your knowledge, expand your understanding, and make you think about how to compete and win in the future. We look forward to you sharing your thoughts and research with us.

—DSK

DISCLAIMER

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.

The Cyber Defense Review

Professional Commentary

The Need for a Cyber Smoke Screen: A Tactical Action that Instantly Becomes Strategic in an All-Domain Operation

Dr. Dan G. Cox

ABSTRACT

Battle space is increasingly transparent. This transparency includes not only electronic signatures but also other actors in the environment. Cell phones today make the movement of military troops and equipment particularly problematic. In order to safely maneuver on the future battlefield, this article proposes the development of a cyber smoke screen. Unfortunately, such a smoke screen, while defensive in nature, would require temporary disruption of local internet and cellular access, thereby bringing this essential defensive maneuver under offensive cyber operations, which implicates both strategic and moral concerns.

INTRODUCTION

As the U.S. military refines its concept for All-Domain Operations (ADO),[1] many new military necessities and problems arise. Preparing for these challenges in advance of prosecuting a war will lead to greater success. This article focuses on a future cyber smoke screen as a pressing example of the complexity of ADO and provides three cogent examples as to why this has become a battlefield imperative. This will be followed by a discussion of related moral and strategic considerations. Finally, the use of a cyber smoke screen is offered to the reader.

WHY A CYBER SMOKE SCREEN IS NEEDED ON THE MODERN BATTLEFIELD

Examining what enemies struggle with on the battlefield is one cogent way to adapt to the future of warfare. The Islamic State in Iraq and Syria (ISIS), the Russian military, and

Dr. Cox has worked with the U.S. Department of Defense and the U.S. Army for seventeen years, including work with U.S. Army Futures Command, the NATO Partnership for Peace Program, improving the professional military education system for the Republic of Armenia's military, and teaching elite military planners operational art and design at the School of Advanced Military Studies (SAMS). He has three published books: *Terrorism, Instability and Democracy in Asia and Africa, Population-Centric Counterinsurgency: A False Idol, and Stability Economics: The Economic Foundations of Security in Post-Conflict Environments*. Dr. Cox is currently researching future warfare, especially issues of cybersecurity, disinformation, the future of design and military planning, and fictional scenarios.

the Ukrainian military have recently demonstrated that cyberspace can be weaponized. And ISIS attempting to stop the weaponization of cyberspace against them failed. Russia too has failed to prevent the weaponization of cyberspace by Ukraine. Still, they seem to have adapted in a way that has prevented further exploitation. As the battlefield becomes more transparent, the need for new ways to hide becomes increasingly important, as illustrated in more detail below.

While ISIS consolidated territorial gains in the Middle East, key leaders became concerned about citizens in controlled areas having access to the internet. ISIS was concerned about online sources leaking information counter to their extreme religious teachings. In the Fall of 2014, ISIS banned all internet access in the key Iraqi city of Mosul.[2] This total ban of the internet in Mosul had disastrous consequences for the local populace. Many local businesses were unable to operate, some services went offline, and residents felt disconnected from the world and their families abroad.[3] ISIS refined its approach in Raqqa, Syria. Instead of banning internet access, ISIS banned private providers but increased the number of ISIS-controlled internet cafes, and even required its own soldiers to use the ISIS-controlled cafes.[4]

As time went on, ISIS continued to control internet access, but they did not again engage in unpopular internet blackouts. Once ISIS realized that the real tactical and operational problem came from cell phones, it began focusing on them. Cell phones not only gave Iraqi and Syrian citizens access to counternarratives, they also could turn these same citizens into sensors, thereby facilitating western forces that were targeting them.[5] While ISIS was able to control broadband, 3G allowed citizens to access the internet and post pictures instantly, which led ISIS again to opt for a total ban on internet access for cell phones.[6] ISIS commandeered all SIM cards, allowing citizens to

take pictures but preventing any sending of text or visual information. Citizens reported feeling as if they had "gone back to the stone age."[7]

Russia's experience with cell phones is more recent and more painful. The most current Russian casualty count with Ukraine is 615,000, with an estimated 115,000 of those forces killed in action.[8] The Russian military is now admitting that many troops were successfully targeted through cell phones.[9] Some of this targeting came through a lack of cell phone discipline. For example, unauthorized use of cell phones by Russian soldiers is the transparent battlefield John Antal warns about, which allowed Ukraine to target a temporarily base of Russian soldiers in Ukraine, resulting in 89 Russian soldiers being killed.[10] More recently, analysts have noted that Russia and Ukraine use cell phone signatures and information aggregators.[11] Antal is correct. The battlefield is becoming more transparent than ever. The idea that masking, the ability to hide maneuvers and formations, is of prime importance.[12]

Open-source aggregation sites further increase battlefield transparency. The website Live Universal Awareness Map (liveuamap.com) began posting conflict information in 2014, and relies on social media, often from freelance reporters and citizens on the ground during conflicts, using embedded geotags to verify the location of social media posts and pictures. "The data is collected by 'AI web crawlers,' which filter relevant stories that are forwarded to a group of expert analysts for fact-checking,"[13] and covers many conflicts, e.g., Ukraine, Gaza, the war in Syria, the war in Afghanistan, ISIS, Al-Qaeda, and Al Shabab.[14] U.S. Marine Corps Lieutenant General (Lt. Gen.) Karsten Heckl noted a growing "ubiquity and proliferation of sensors" on the battlefield.[15] Lt. Gen. Heckl notes that battlefield sensors increasingly allow for a quick and effective targeted kill.[16] Both Russia and Ukraine have suffered losses from the latest mobile, intelligence-driven sensors: humans with cell phones. AI-driven aggregators of social media posts will only exacerbate this danger to maneuvering forces.

A more recent incident brings the need for a cyber smoke screen into sharp focus. On September 17 and 18, 2024, Israel conducted stunning attacks against Hezbollah leadership and operatives.[17] The attacks resulted in dozens of Hezbollah operatives killed and thousands more wounded.[18] Hezbollah had recently ordered new pagers and walkie-talkies as to which Israel had infiltrated the production chain, embedding small explosive charges into each device.[19] These attacks make cell phone-enabled Improvised Explosive Device (IED) attacks in Iraq and Afghanistan against U.S. soldiers look archaic by comparison. One can imagine a future battlefield where multiple cell phone-enabled explosives line logistical routes making the need for a cyber smoke screen even greater.

Hiding, camouflage, and other masking techniques remain critically important. Future battlefields likely will become increasingly more dispersed than battlefields of the past. Still, large and small formations will have to traverse the transparent battlefield, and militaries will be able, when opportune, to mass or converge on opposing units. Logistical supply must also traverse dangerous battlefields. All the operational movements on the battlefield will

require the ability to thwart as many sensors as possible and one of the most effective sensors on today's battlefield is the cell phone-armed person on the ground, thereby enhancing the need for a cyber smoke screen, the implementation of which is discussed below. Simply put, an effective cyber smoke screen will serve to temporarily arrest internet functionality and cellular services for just long enough to allow military units safe maneuver without detection.

THRESHOLD CHALLENGES IN IMPLEMENTING A CYBER SMOKE SCREEN

The need for cyber smoke screens is clear and, as discussed below, implementing this raises ethical and other strategic challenges. The final section of this article proposes ways to employ cyber smoke screens that address and accommodate some of these challenges.

When ISIS shut down internet access for the people of Mosul for an extended period, it likely violated International Humanitarian Law (IHL). No specific IHL governs cyberspace, but corollary IHL rules do govern the denial of water or food. IHL governing *jus in bello*, or the just prosecution of war, provides a framework for boundaries that should guide militaries in modern warfare.

Capturing both the IHL inherent in the Geneva Accords and expanding the notions to modern war, Michael Walzer's book, *Just and Unjust Wars*,[20] provides a good starting point for this discussion. Walzer's concept of proportionality and double effect are particularly apt here. Walzer lays out the principle of double effect as a common occurrence in war whereby normal and necessary military operations often put non-combatants at risk or in harm's way. The military action has the double effect of being a good, legitimate, and military necessary action in war, yet unintentionally harmful to innocent civilians.[21] Walzer lists four criteria for a just action in a war that poses a high risk of double effect. Of these, the fourth criterion, "proportionality," is particularly pertinent to this discussion. Walzer argues, "the good effect [must be] sufficiently good to compensate for allowing the evil effect."[22] In other words, the harm befalling civilians must be less than the military benefit or necessity.

The Geneva Conventions echo the concepts of "proportionality" and "military necessity." Article 3 requires that non-combatants, including prisoners of war, be treated as humanely as possible.[23] Article 53 deals explicitly with military necessity, and prohibits destroying civilian property unless compelling and necessary for military operations.[24] These two prohibitions on harm to civilians and civilian property nest nicely with aspects of civilian life that should never be intentionally disrupted, regardless of military need, such as water or food. IHL renders the disruption of water supplies to civilians an explicit war crime.[25] IHL on cyberspace remains to be developed, but clearly, while the internet is vital to a modern functioning society, it is nowhere near as pressing as the human need for water and food. Still, caution and mindfulness are essential when military necessity requires large-scale and prolonged disruption of internet services.

Reviewing the ISIS ban on the internet is instructive here. The ban was instituted for two reasons. First, ISIS did not want foreign ideas to infiltrate their caliphate. Second, ISIS leaders worried that geo-location tags on pictures from cell phones and other social media posts would help Iraqi and Western military operators target key leadership more effectively.

The first reason for internet disruption hardly fits the definition of military necessity, but the second reason – avoiding targeting bulls-eyes – clearly fits. However, enforcing that ban by ISIS was both disproportional and also a war crime. When ISIS detained and burned alive citizens in Mosul caught with a cell phone sim card,[26] the military necessity rationale was clearly overwhelmed by the proportionality guard rails of IHL.

Further, a blanket denial of internet access for months or years caused such significant economic and psychological damage to the citizens of Mosul that it would violate Walzer's notion of double effects in war if the harm to civilians outweighed the military benefit of the operation. Even in terms of effectiveness, disruption of internet services in Mosul seems counterproductive. From a simple counterinsurgency standpoint, cutting off civilians from the internet for a prolonged period undoubtedly cause deep resentment against the occupying forces. Minimizing that resentment is a factor the U.S. should keep in mind in future military operations.

Beyond these moral considerations, cyber smoke screens pose other strategic complexities, such as the way U.S. Cyber Command (USCYBERCOM) is organized with offensive and defensive cyber operations (OCO/DCO) separated as siloed and distinct entities creates further problems.[27] So far there is much less analysis of OCO in the literature, and most U.S. cyber operations remain defensive in nature.[28] USCYBERCOM expanded its notion of cyber operations in 2018, but this all was mainly aimed at expanding defensive operations. In 2018, the notion of defending forward came into vogue. Instead of simply defending the homeland, USCYBERCOM would now partner and help allies defend from cyberattacks from adversaries, ensuring that forces and capabilities of allied nations' military and infrastructure assets and U.S. military assets abroad remained safeguarded.[29]

Even in a predominantly defensive role, USCYBERCOM realizes that the innate interconnected nature of cyberspace means that the U.S. will be in constant contact with adversaries and enemies. Therefore, defending forward is married with the notion of persistent engagement in cyberspace. However, this persistent nature is almost exclusively defensive in nature. An Offensive Cyber Operation (OCO) will mainly occur either to prevent an attack or during a war. Even during a war, OCO authorities still largely reside at the Strategic level, mainly with the U.S. president.[30]

There are compelling reasons why OCO is so hard to enact. The authorities for OCO are held at the highest level in the United States. As Austin Long notes, it takes guidance from the National Command Authority (NCA) to develop potential strategic OCO, and no known directives or authorities exist at the operational or tactical level.[31]

What is ironic about this current article is that what seems to be, on the surface, a defensive cyber operation, a cyber smoke screen, is also immediately offensive. Military operators will have to disrupt local internet networks to establish the cyber smoke screen and effectively mask military maneuvers. ISIS, Russia, and Ukraine have all been negatively affected by using cell phones on the ground. The advent of aggregator websites like Liveuamap makes the need for masking movement from people with cell phones even more pressing.

CYBER SMOKE SCREENS FOR FUTURE WAR

The need for masking military maneuvers is only going to grow over time. Assuming authorities for at least limited OCO will be pushed down to the operational and tactical levels, what should a moral and operationally sound cyber smoke screen look like?

As to moral implications, some international legal scholars likely will argue that internet access is like water and, hence off limits even in war. But the internet arguably is not a basic need. While integral to modern economic activity, it can be disrupted. The debate more properly should be focused on duration, and not the consequences of an indefinite disruption of internet services. The military necessity of a cyber smoke screen is compelling. Military maneuvers are too risky to conduct with millions of sensors on the ground constantly compromising positions via civilian cell phones. This does not mean it is militarily prudent or morally correct to follow the spirit of IHL to disrupt internet and cell phone services broadly for a prolonged period.

Instead, a cyber smoke screen would comprise a temporary disruption of the internet and cell phone services (several hours at most) to allow military units to maneuver through the terrain, especially urban areas, without showing up on aggregation websites and targeting schemes of enemy forces.

A single cyber smoke screen along one route will be insufficient since the outage trajectory itself might give the enemy a good idea of where forces are headed. Therefore, two or more cyber smoke screens may need to be deployed simultaneously to deceive and present a dilemma to enemy forces and prevent or at least greatly diminish the opportunity to mass on U.S. forces. Each cyber smoke screen would take a distinct and significantly different route through the terrain. Two would be fakes and one would mask the real military movement. This tactic would increase the chance of successfully moving through an area undetected while reducing the risk of movement. Human intelligence could easily thwart this system, but cell phones would be mitigated as a means of exposure.

This means that USCYBERCOM must accelerate its mixing of offensive and defensive cyber operations. The notion of a cyber smoke screen also illustrates the dual and simultaneous nature of many necessary tactical and operational cyber operations. This means that USCYBERCOM must be given more authorities for OCO, which it has to push down to the operational

and tactical level. Further, USCYBERCOM must reintegrate OCO and DCO operations and units as they recognize that cyberspace does not easily fit into separate silos of offense and defense. Failure to adapt means U.S. troops will be exposed to the risk of being placed in a quick-kill chain by the enemy.

DISCLAIMER

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, the School of Advanced Military Studies, the Department of the Army. or the Department of Defense.

NOTES

1. It should be noted that joint publications refer to ADO, but U.S. Army doctrine refers to Multi-Domain Operations (MDO) which means basically the same thing. Department of the Army. *FM 3.0 Operations*, (October 2022).
2. Associated Press, "ISIS Blocks Mobile Phone Networks in Largest City They Control," (November 27, 2014). AP Report on *CBS News Online*, https://www.cbc.news.com/news/isis-blocks-mobile-phone-networks-in-mosul./.
3. Associated Press, "ISIS Blocks Mobile Phone Networks in Largest City They Control."
4. Al Jazeera, "ISIL Bans Private Internet Access in Syria's Raqqa," (July 20, 2015). *Al Jazeera News Online*, https://www.aljazeera.com/news/2015/7/20/isil-bans-private-internet-access-in-syrias-raqqa.
5. Benjamin Plackett, "Burned Alive for Using a Smartphone," (Updated April 5, 2019). *Engadget Online,* (https://www.engadget.com/2019-04-05-isis-mosul-occupation-killed-for-smartphone.html.
6. Benjamin Plackett, "Burned Alive for Using a Smartphone."
7. Benjamin Plackett, "Burned Alive for Using a Smartphone."
8. Eric Schmitt, "September Was Deadly Month for Russian Troops in Ukraine, U.S. Says," (October 10, 2024). *The New York Times*, https://www.nytimes.com/2024/10/10/us/politics/russia-casualties-ukraine-war.html.
9. Helene Cooper, Thomas Gibbons-Neff, Eric Schmitt, and Julian E. Barnes, "Troop Deaths and Injuries in Ukraine War Near 500,000, U.S. Officials Say," (August 18, 2023). *The New York Times*, https://www.nytimes.com/2023/08/18/us/politics/ukraine-russia-war-casualties.html.
10. Colonel (Retired) John Antal, *7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting.* (February 3, 2022). New York: Casemate, 4; and Felipe Dana, "Russia Says Phone Use Allowed Ukraine to Target Its Troops," (January 4, 2023). *Associated Press,* https://www.military.com/daily-news/2023/01/04/russia-says-phone-use-allowed-ukraine-target-its-troops.html.
11. Chris Stokel-Walker, "Russia and Ukraine are Both Weaponising Mobile Phones to Track Troops," (April 11, 2022). *New Scientist*, https://www.newscientist.com/article2315553-russia-and-ukraine-are-both-weaponising-mobile-phones-to-track-troops/.
12. John Antal, *7 Seconds to Die: A Military Analysis of the Second Nagorno-Karabakh War and the Future of Warfighting*, 143.
13. *European Union Data Portal,* "Live Universal Awareness Displays Events Related to Russia's Invasion of Ukraine." (May 27, 2022). https://data.europa.eu/en/news-events/news/live-universal-awareness-map-displays-events-related-russias-invasion-ukraine.
14. Liveuamap, LLC, *Live Universal Awareness Map*, (June 9, 2024). API operated from McLean, Virginia using European Union Infrastructure, https://liveuamap.com.
15. John M. Doyle, "General: Precise Sensors to Close Kill Chain Is a Key Takeaway from Ukraine," (May 5, 2022). *Seapower Magazine*, https://seapower.magazine.org/general-precise-sensors-to-close-kill-chain-is-a-key-takeaway-from-Ukraine.
16. John M. Doyle, "General: Precise Sensors to Close Kill Chain Is a Key Takeaway from Ukraine."
17. Kat Lonsdorf and Itay Stern, "From pager blasts to Nasrallah's killing: 12 days that transformed a bloody conflict." (September 29, 2024). *NPR*. (accessed Oct 5, 2024). https://www.npr.org/2024/09/29/g-s1-25348/israel-hezbollah-lebanon-hassan-nasrallah-timeline.
18. Matt Murphy, "What We Know About the Hezbollah Device Explosions," (September 20, 2024). BBC News. (Accessed October 5, 2024). https://www.bbc.com/news/articles/cz04m9l3m49o.
19. Jonathan Yerushalmy and Dan Milmo, "Hezbollah device blasts: how did pagers and walkie-talkies explode and what do we know about the attacks?" (September 18, 2024). *The Guardian*. (accessed October 5, 2024). https://www.theguardian.com/world/2024/sep/18/hezbollah-pagers-what-do-we-know-about-how-the-attack-happened.
20. Michael Waltzer, Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, (1977). New York: NY: Perseus Books Group: 152-53.
21. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 152-153.
22. Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, 152-153.
23. *Geneva Convention Relative to the Protection of Civilians in Time of War. 12 August 1949. Article 3, Conflicts Not of an International Character,* (June 7, 2024). Geneva: International Committee of the Red Cross, International Humanitarian Law Databases, https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-3.

NOTES

24. *Geneva Convention Relative to the Protection of Civilians in Time of War. 12 August 1949. Article 53, Prohibited Destruction*, (June 7, 2024). Geneva: International Committee of the Red Cross, International Humanitarian Law Databases, https://ihl-databases.icrc.org/en/ihl-treaties/gciv-1949/article-53.
25. Peter H. Gleick, "It's Vital to Protect Water Infrastructure During War," (June 7, 2023). *Time*. https://time.com/6285314/ukraine-dam-destruction-water-war-essay/.
26. Benjamin Plackett, "Burned Alive for Using a Smartphone."
27. U.S. Cyber Command Public Affairs, "Cyber 101 – Cyber Mission Force," (November 1, 2022). https://www.cybercom.mil/Media/News/Article/3206393/cyber-101-cyber-mission.
28. Austin Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning." (February 18, 2017). *Journal of Cybersecurity*. Issue 3, No. 1, https://academic.oup.com/cybersecurity/article/3/1/19/3003367, 19.
29. Nina Colliers and Jacquelyn Schneider. "Defending Forward: The 2018 Cyber Strategy is Here," (September 20, 2018). *War on the Rocks*, https://waronthrocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/.
30. Michael P. Fisherkeller and Richard J Harknett, "Persistent Engagement, Agreed Competition, and Cyberspace Interaction Dynamics and Escalation," (December 9, 2019). *The Cyber Defense Review, Special Edition, International Conference on Cyber Conflict* (CYCON U.S.), 269-70.
31. Long, "A Cyber SIOP? Operational Considerations for Strategic Offensive Cyber Planning," 20.

The Cyber Defense Review

Research Articles

The Path to China's Intelligentized Warfare: Converging on the Metaverse Battlefield

Josh Baughman

ABSTRACT

The People's Liberation Army (PLA) modernization strategy follows three overlapping phases: mechanization, informatization, and intelligentization. Mechanization, aimed to be broadly completed by 2020, focused on incorporating advanced machinery, vehicles, and equipment. The informatization phase introduced networks, information systems, and data to all aspects of military operations, including command and control, intelligence, surveillance, and reconnaissance (ISR), and cyber operations. Since 2019, while still pursuing the aims of informatization, intelligentization endeavors to incorporate emerging technologies such as artificial intelligence (AI), quantum, big data, virtual and augmented reality, cloud computing, autonomous systems, and the internet of things (IoT). Recent PLA writings describe the culmination of intelligentization as leading to "Metaverse War" (元战争), or Meta-War. In this vision, the metaverse becomes central not only to China's broader societal transformation under "Digital China" (the world's first digital grand strategy)—which aims at "winning the future"—but also a defining feature of future warfare. PLA literature has extensively explored building a military metaverse (战场元宇宙), or "battleverse," and is now focused not only on how metaverse wars will be fought, but also how they will be won spanning both near- and long-term time horizons.

Joshua D. Baughman ("Josh") currently serves as an analyst at the Air University's China Aerospace Studies Institute (CASI). His research centers on China's People's Liberation Army (PLA) activity in the cyber and information domain and the PLA Rocket Force. He guest-lectures at the National Defense University, Institute of World Politics, and Foreign Service Institute, in both masters- and doctoral-level courses, on topics such as China's cyber strategy and cognitive domain. He presents and publishes regularly and has received international recognition for his work on the metaverse. Josh previously worked at National Defense University (NDU) College of Information and Cyberspace (CIC), the U.S. Air Force Academy, and Tsinghua University in Beijing. Collectively, he spent three years living in Beijing working as an editor and journalist on China security issues, as well as a television host, director, writer, and producer. In his spare time, Josh volunteers for the Military Cyber Professionals Association, a 501(c) (3) educational nonprofit charity, as part of national leadership as the Chief Marketing Officer. Josh is professionally proficient in Mandarin.

INTRODUCTION

The People's Liberation Army's military modernization strategic framework, as articulated by high-ranking officials, including the People's Republic of China's (PRC's) supreme leader Xi Jinping, is structured around three distinct yet overlapping phases: mechanization, informatization, and intelligentization. Mechanization refers to the incorporation of advanced machinery, vehicles, and equipment into the PLA, a process intended to be largely completed by 2020. The next phase shifted focus toward informatization, which involves the integration of information systems, networks, and data into all aspects of military operations, including command and control (C2), intelligence, surveillance, and reconnaissance (ISR), and cyber operations. The final phase, first mentioned in 2019, is intelligentization, which envisions the transformative impact of advanced technologies on 21st-century warfare. This framework embodies China's conceptualization of a new revolution in military affairs. The PRC's 2019 white paper, *National Defense in the New Era*, underscores that emerging technologies such as artificial intelligence (AI), quantum, big data, virtual and augmented reality, cloud computing, autonomous systems, and the internet of things (IoT) signify a shift in warfare to a new "intelligentized" era.[1] In more recent writings, PLA authors see the culmination of intelligentization as leading to what they call Metaverse War [元战争] (also known as Meta-War). For the PLA, the metaverse will be the defining feature both for society as they pursue a digital grand strategy known as Digital China[2] with the stated goal of "winning the future" and for warfare. While much has been written in PLA literature about how to build a military metaverse [战场元宇宙] (also known as the battleverse),[3] the PLA is now defining not only how metaverse wars will be fought, but also how they will be won in near and far future conflicts.

DEFINING META-WAR

While the focus of the metaverse, both in China and globally, has been on civilian use with production, entertainment, and general life enhancement, the PLA has been working on strategic ideas for military application. Initially, the military application of the metaverse was introduced in Chinese media through an article titled "Uncovering the Metaverse" published in the *PLA Daily* in November of 2021.[4] The article proposed utilizing the metaverse to depict the horrors of war as a means of deterring conflict. The authors suggested that "if news reports could recreate the scenes of war and establish a 'battleverse,' it would allow individuals to experience, in real time, the immense trauma war inflicts on human civilization. This shock could potentially foster a greater societal interest in peace." In this context, the metaverse is envisioned not as a military tool, but rather as a means for civilians to comprehend the profound impact of warfare on human lives.

In a matter of months, the dialogue around the metaverse in the PLA changed to one in which they explored how to build and utilize a separate military metaverse (also known as the battleverse) to win future intelligentized war. PLA articles explored how to build a military metaverse and possible ways to disrupt an adversary's ability to use their own military metaverse. In the most recent PLA article on the metaverse titled "Meta-War: An Alternative Vision of Intelligentized Warfare," authors Zhang Yuantao, Luo Yanxia, and You Xiaotong continue the conceptualization of future wars and argue that intelligentized warfare inevitably leads to meta-war. They define meta-war as, "a new type of military activity that uses military confrontation as the main means to conquer the opponent's will and realize one's own goals by utilizing politics, economics, and social interaction supported by metaverse technology."[5] From a technical standpoint, meta-war refers to a battlefield "super system" [超系统] created through the integration of brain-computer interfaces, smart devices, and virtual, augmented, and mixed reality technologies. This system interacts with various weapon platforms and military forces on the actual battlefield, connecting everything to form a fully interconnected and integrated combat environment. From a combat perspective, meta-war links the physical battlefield, the virtual battlefield, and the "brain battlefield" [头脑战场], which represents the conscious perceptions of officers and soldiers. This system enables deep, multi-modal interaction with a wide range of targets on the battlefield. It allows officers and soldiers to seamlessly switch between the real-world battlefield and a virtual parallel battlefield as needed, enabling them to engage in combat, simulate war scenarios, and predict outcomes in an immersive environment.

COMBAT METHODS

The authors of "Meta-War: An Alternative Vision of Intelligentized Warfare" perceive three methods of combat in meta-war including "(Virtual) Clone/Avatar [分身] Combat in the Virtual World", "Simulacrum/Imitation [仿身] Combat in the Real World," and "Incarnation/Embodiment [化身] Combat in Parallel Worlds" as shown in Table 1.

Meta-War Combat Methods	Description
(Virtual) Clone / Avatar [分身] Combat in the Virtual World	Military operations conducted in a virtual environment created within the meta-battlefield.
Simulacrum / Imitation [仿身] Combat in the Real World	Real-world combat in which weaponized "simulacrums" are deployed to fight in place of humans.
Incarnation / Embodiment [化身] Combat in Parallel Worlds	Combines the first two concepts with human, avatar, and simulacrum working in unison.

Table 1. Possible Combat Methods in a Metaverse War.

"(Virtual) Clone/Avatar Combat in the Virtual World" refers to military operations conducted in a virtual environment created within the meta-battlefield, involving activities like cyber warfare, simulated combat, and training exercises. Combatants influence networks, public opinion, and other factors behind the scenes to carry out military interventions, while using virtual avatars on the front lines to conduct pre-battle training, prepare for deployment, and engage in combat. The authors give the example of the film *Ready Player One* in which the protagonist enters the virtual world "OASIS" (Ontologically Anthropocentric Sensory Immersive Simulation) using VR glasses. As the top player in the OASIS, he leads his team through various challenges and ultimately collects the three keys needed to win the game. While battles take place in the real world, final victory is determined by who first discovers the hidden keys within the virtual world.

"Simulacrum/Imitation Combat in the Real World" refers to real-world combat in which weaponized "simulacrums" are deployed to fight in place of humans. Simulacrum, like the word simulation, comes from the Latin verb *simulare* which means to copy, represent, or feign. A simulacrum is a representation or imitation of a person, object, or concept. In contemporary usage, it often refers to a copy or reproduction that has become disconnected from its original source, playing a significant role in areas such as philosophy, art, and media studies. These simulacrums carry human perception and intent, allowing them to perform dangerous and complex tasks on behalf of their operators. They may take the form of humanoid robots, bionic robots, or mechs, controlled in real time by humans using brain-computer interfaces, remote controls, or tactile devices. They can function in various configurations, including team-based, modular, or integrated systems. While under human oversight, these simulacrums are capable of autonomously planning and executing combat actions. The authors give the example of Tesla's "Optimus" humanoid robot, which incorporates Tesla's AI system for network-based learning and possesses advanced scene perception and real-time decision-making skills. The PLA is currently looking seriously into the application of humanoid robots in future warfare.[6]

"Incarnation (or Embodiment) Combat in Parallel Worlds" in essence combines the first two concepts with human, avatar, and simulacrum working in unison. Human soldiers and their weapons on the battlefield function as dual entities, existing both in the physical world and as digital twins,[7] capable of switching between and interacting across multiple parallel realities.

Virtual objects in the battlefield correspond to real-world counterparts, allowing humans to control virtual weapon platforms or issue commands to real-world systems. The outcome of battles is ultimately determined by the interaction of physical entities. For example, in the movie *Infinite*, the antagonist uses a fingertip controller to deploy virtual drone swarms within a 3D holographic display, controlling them through gestures. The real drone swarm, mapped to its virtual counterpart, then carries out attacks in the physical world.

WINNING THE META-WAR

As traditional warfare in the physical world approaches its limits, virtual combat domains—enabled by technologies like virtual reality—have emerged. The shift from separating virtual and physical combat environments to integrating and connecting them will progressively drive the evolution and advancement of meta-war. Effectively integrating physical and virtual in future wars will be a key component in achieving victory over an adversary. The authors suggest three possible strategies for winning future meta-wars: Decoupling and Splitting [解耦裂变], Intelligent Evolution [智能演化], and Mirror War [镜像战争].

How to Win the Meta-War	Description
Decoupling and Splitting [解耦裂变]	A software-based integrated combat system which will enable a transformation of the battlefield from just physical to virtual environments.
Intelligent Evolution [智能演化]	Enhancement of decision making and cognition with the synergy of human intelligence, machine intelligence, biological intelligence, network empowerment, and the combined effect of parallel virtual-real platforms.
Mirror War [镜像战争]	Subduing the opponent's will in virtual environments without resorting to large-scale physical warfare.

Table 2. Strategy for Winning a Metaverse War.

"Decoupling and Splitting" focuses on moving towards a "software-based integrated combat system" which will enable a transformation of the battlefield from just physical to virtual environments. This shift will decouple hardware from software, introducing a software-defined combat model. The continuing evolution of the internet, IoT, and other emerging technology are creating an intelligent interconnection of all systems. With this interconnection the various aspects of meta-war can either be physically deployed in the real world or pre-programmed within virtual network environments. These elements can be controlled by humans using multi-modal interfaces, such as voice, visual, touch, or brain computer interface (BCI), allowing for interactive management of networked weapon platforms.

"Intelligent Evolution" emphasizes the enhancement of decision making and cognition with the synergy of human intelligence, machine intelligence, biological intelligence, network empowerment, and the combined effect of parallel virtual-real platforms. "Decision-Centric Warfare" [决策中心战] is a concept the PLA has studied from the United States (U.S.) military.

They believe that by supporting advanced technologies such as artificial intelligence, diversified tactics achieved through the upgrading and transformation of combat platforms, and distributed deployment they can "accelerate cognition."[8] Another U.S. military concept studied by the PLA, "Mosaic Warfare," also falls under "Intelligent Evolution." Dr. Thomas Burns, the retired Director of DARPA's Strategic Technology Office, defines the term, "The idea will be to send so many weapon and sensor platforms at the enemy that its forces are overwhelmed. The goal is to take complexity and to turn that into an asymmetric advantage."[9] While ensuring one's own tactical selection advantages, high complexity is imposed on the enemy to interfere with its command and decision-making capabilities, thereby achieving an overwhelming advantage over the enemy.

"Mirror War" looks much farther into the future in which the boundary between real-world warfare and virtual warfare becomes indistinguishable. The end goal is to achieve victory by subduing the enemy without fighting. Classical war theories that include war as inherently violent could be changed as war would cease to happen in physical reality. The approach involves virtually mapping the military and national power of both combatants, following the principles of meta-war. The conflict is simulated through non-violent mirror projections, aimed at persuading or subduing the opponent's will without resorting to large-scale physical warfare. If there is no distinction between physical and virtual, a loss in the virtual equates to a loss in the physical. Of course, as the authors point out, many forms of deception could be used to convince the adversary of greater capability than what is believed.

FIRST META-WAR?

Professor of Political Science and International Relations and Director of the World Politics Research Center at China Foreign Affairs University, Shi Zhan, argues in his recent work "The First Metaverse War"[10] that the Russian-Ukraine War could be considered a "beta version" of meta-war.[11] With networked communication, such as social media, war has become a more personal experience as images from the battlefield can be transmitted directly to individuals' smartphones without the need for government or media mediation. Through social media on personal devices, civilians can be a part of war as they share their thoughts, ideas, and highlight narratives they believe to be true. For the Ukraine civilians at or near the battlefield, Ukraine's Ministry of Digital Transformation set up the eVorog ("eEnemy") chatbot in March 2022, just weeks after Russia invaded.[12] The chatbot, accessible via smartphone, guides users through a series of questions to determine what they witnessed, as well as where and when it occurred. Hosted on the encrypted messaging platform Telegram, the interface uses the government app Diia to verify the identity of those submitting information. The phone's satellite navigation feature confirms the user's location. This "gamification" on the network for Ukraine civilians helps encourage everyone to be a part of the war where digital (smartphone app) and physical (perceiving physical activities of the Russian army) meet.

Furthermore, Professor Shi Zhan writes that Volodymyr Zelenskyy has the ability to shape narrative in virtual space. He argues that while Zelenskyy is located in Kyiv, he can still effectively address the U.S. Congress, the European Parliament, and other international bodies, rallying immense support without leaving the capital. This blend of virtual communication and real-world presence mirrors a metaverse-like integration of online and offline realities.[13] A video released after his speech to the U.S. Congress juxtaposed Kyiv's pre-war beauty with its wartime devastation, set to poignant music.[14] The artistic presentation powerfully conveyed the tragedy on a global scale.[15] Vladamir Putin, in contrast, lacks the same performative and narrative ability to integrate offline and online support and generate supporters on the network, a perspective Professor Shi Zhan views as a metaphor for the metaverse.

FUTURE AHEAD

While the metaverse is still in its infancy, we can already see the foundational technologies of the metaverse playing a critical role in current conflicts such as with Ukraine and Russia. The Chinese Communist Party (CCP) and the PLA they have a stated goal of achieving the "innovation high ground" and "winning the future." Intelligentization can be seen as the military framework of this aim. The CCP understands the power of technological superiority on the battlefield and thus, have positioned themselves to be the leader of the metaverse. It can be seen as dual use, both to elevate their society and economy while also being utilized in warfare. The CCP believes if they can create a first mover advantage in the metaverse they will be the dominant force of the future. Special Competitive Studies Project (SCSP)[16] CEO Ylli Bajraktari warns in a recent keynote at the National Defense University College of Information and Cyberspace Cyber Beacon Conference, "The digital footprint could be controlled by China in the future." However, the metaverse will not be built by one country alone. The United States' greatest advantage is our allies and partners. We must continue to leverage not only our own indigenous capabilities by cultivating and investing in talent, but also work with our allies both in the public and private sector to secure the advantages that the metaverse will bring both for the military and all of society. At the heart of intelligentization and meta-war is to conquer the opponent's will to fight. For the United States and our allies and partners we must not only prepare our military, but also civilians, because in metaverse wars, we all have a role to play as the lines between real and virtual continue to converge.

DISCLAIMER

The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of the Air Force, or the Department of Defense.

NOTES

1. The State Council, "Full Text: China's National Defense in the New Era," (Accessed October 16, 2024). The People's Republic of China, https://english.www.gov.cn/archive/whitepaper/201907/24/content_WS5d3941ddc6d08408f502283d.html.
2. To learn more about Digital China read "Translation: Plan for the Overall Layout of Building a Digital China," https://digichina.stanford.edu/work/translation-plan-for-the-overall-layout-of-building-a-digital-china/.
3. To learn more about how China will build a battleverse see "Enter the Battleverse: China's Metaverse War," https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1083&context=mca.
4. Dai Binxiong [戴斌熊], Xiong Sunhao [雄孙浩], "Uncovering the Metaverse" [揭开'元宇宙'面纱], (Accessed March 9, 2022). http://www.81.cn/jfjbmap/content/2021-11/26/content_303934.htm.
5. Zhang Yuantao [张元涛], Luo Yanxia [落焱霞], and You Xiaotong [尤晓彤], "Meta-War: An Alternative Vision of Intelligentized Warfare" [元战争：智能化战争的另类推], (Accessed September 10, 2024). China Ministry of National Defense Network [国防部网], http://www.81.cn/szb_223187/szbxq/index.html?paperName=jfjb&paperDate=2024-09-10&paperNumber=07&articleid=939348.
6. Wang Yonghua [王永华], "Pay Attention to the Military Application of Humanoid Robots" [关注人形机器人军事运用], (Accessed July 1, 2024). China Ministry of National Defense Network [国防部网], http://www.81.cn/szb_223187/szbxq/index.html?paperName=jfjb&paperDate=2023-06-13&paperNumber=07&articleid=908058.
7. To learn more about PLA's work on digital twins read: "Enhancing the Battleverse: The People's Liberation Army's Digital Twin Strategy," https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1091&context=mca
8. Hu Xiaofeng [胡晓峰], "Complexity Is Also a Weapon" [复杂性也是一种武器], (Accessed October 16, 2024). China Ministry of National Defense Network[国防部网], htttp://www.81.cn/szb_223187/szbxq/index.html?paperName=jfjb&paperDate=2023-07-04&paperNumber=07&articleid=909584.
9. Defense Advanced Research Projects Agency (DARPA), "DARPA Tiles Together a Vision of Mosaic Warfare," (Accessed October 16, 2024). Arlington, VA: DARPA. https://www.darpa.mil/work-with-us/darpa-tiles-together-a-vision-of-mosiac-warfare.
10. Shi Zhan, "The First Metaverse War," (Accessed September 15, 2024). Reading the China Dream, https://www.readingthechinadream.com/shi-zhan-the-first-metaverse-war.html.
11. It is also being called the first commercial space war, the first full-scale drone war, and the first AI war.
12. Valeriya Ionan, "Delivering Digital Transformation in Ukraine," (Accessed November 15, 2024). Chandler Institute of Governance, https://www.chandlerinstitute.org/governancematters/delivering-digital-transformation-in-ukraine.
13. Shi Zhan, "The First Metaverse War."
14. *Zelensky Gets Standing Ovation after Speech to Congress*, 2022. https://www.youtube.com/watch?v=RZ_ykL6QJE0.
15. Shi Zhan, "The First Metaverse War."
16. SCSP's mission is to make recommendations to strengthen America's long-term competitiveness as artificial intelligence (AI), and other emerging technologies are reshaping our national security, economy, and society. https://www.scsp.ai/.

Allegations of U.S. Cyber Hegemony Complements China's Influence Campaign

to Weaken Global Confidence in the United States

Emilio Iasiello

ABSTRACT

The People's Republic of China (PRC) has engaged in an aggressive media campaign, using classified data leaks exposing controversial United States (U.S.) cyber activities to paint it as a cyber hegemon. This effort has dovetailed with other influence operations in an effort to frame the U.S. as an untrustworthy global partner motivated by its own self-interests ahead of the global community. The U.S. Department of State released a recent report on these activities, correctly concluding that they have had questionable successes. However, the PRC is using these campaigns not so much as to supplant the U.S. as a global leader, but rather to keep it in check by raising questions in the minds of those nations not already bound to the U.S. to not blindly follow Washington's lead. The PRC seeks to capitalize on this to press forward on core political and economic issues, which if achieved, could put the PRC closer to its goals as an influencing global leader.

Keywords: *Cyber, China, Cyber Hegemony, Influence Campaign*

INTRODUCTION

Over the past year, the PRC has engaged in an antagonistic media campaign criticizing U.S. global cyber activities as hegemonic, designed to exert undue influence and dominance over the Internet domain to advance its interests as the world's preeminent cyber leader. Via its state-controlled online media channels, the PRC has leveraged classified data leaks and the U.S.'s "defend-forward" cyber strategy to buttress the narrative describing the U.S. as a hypocritical nation, driven solely

Emilio Iasiello has more than twenty years of experience as a strategic cyber intelligence analyst, supporting U.S. government civilian and military intelligence organizations, as well as the private sector. He has delivered cyber threat presentations to domestic and international audiences and has published extensively in such peer-reviewed journals as *Parameters*, the *Journal of Strategic Security*, the *Georgetown Journal of International Affairs*, and West Point's *The Cyber Defense Review*, among others.

by self-interest, and guilty of the very activities it attributes to other nations. This media blitz dovetails with other PRC information campaigns that seek to discredit the U.S. with respect to other issues, such as military support for Ukraine and Israel, thereby framing Washington as a government that pervasively interferes in other state's affairs. This aggressive position, driven by Xi Jinping, stands in stark contrast to the more passive approach under Hu Jintao and the peaceful development strategy aimed to mitigate conflict as the PRC achieved its objectives gradually. Xi no doubt perceives a U.S. that is weakened by internal political division,[1] back-seated to a secondary role in world affairs, and less able to drive foreign policy. To capitalize on this, Xi appears to envision more maneuverability on the world stage to pursue the PRC's global aspirations.

THE PRC KEEPS LIGHT ON QUESTIONABLE U.S. CYBER ACTIVITIES

In response to allegations from cybersecurity companies and foreign governments over its pervasive offensive cyber operations, the PRC has issued official denials, citing its own victimization at the hands of malicious attackers.[2] In response to accusations from victims, the PRC stubbornly demands proof of such claims.[3] It was only after repeated U.S. accusations citing the PRC as a prominent cyber threat in its unclassified threat assessments, coupled with the 2020 Chinese cybersecurity company Qihoo 360 attributing hostile cyber activity since 2008 to the U.S. Central Intelligence Agency (CIA),[4] that the PRC shifted its tack. This 2020 shift by the PRC upgraded its passive "deny, deny, deny" strategy with a more offensive attack, seeking to expose U.S. cyber malfeasances and neutralize U.S. success in leveraging the U.S. cybersecurity community to publish and disseminate findings of a foreign government's cyber operations.

The 2020 Qihoo 360 report marks the beginning of PRC efforts to expose U.S. cyber surveillance and

operational activities, and thereby paint the U.S. as the premier cyber threat to the global community, letting the world know that the PRC too is capable of tracking highly sophisticated threat actors operating in cyberspace. Several state-controlled and/or influenced PRC media sources such as the *Global Times*, *South China Morning Post*, and *China Military* since 2020 have published accusations in efforts to "name and shame" alleged U.S. cyber campaigns in an attempt to expose the U.S. and otherwise shift attention. Notable articles have highlighted incidents where the U.S. has allegedly conducted the types of activity that it has accused the PRC of doing.

Themes	Chinese Media "Naming and Shaming" Campaigns
Recruiting Insiders to Support Cyberspying	In November 2023, the PRC's Ministry of State Security (MSS) reported an investigation involving the recruitment of a Chinese software developer that provided "technical services" to a foreign spy agency. The spy agency had corrupted the software to conduct cyberattacks and steal information from several of Chinese defense and high-tech organizations, according to the *Global Times*.[5] While the U.S. was not specifically named in the article, the innuendo was that the expertise and sophistication was telltale.
Internet Governance	In November 2023, the *Global Times* took the lead in condemning the U.S. as a cyber hegemon, in stark contrast the the PRC's vision of a shared future in cyberspace underpinned by joint contribution, shared benefits, and collective resolution of security challenges,[6] and otherwise condemning perceived U.S. hegemonic practices of global surveillance, building cyber arsenals, coercing governments to thwart PRC telecommunications, and massive data theft.[7]
Huawei Enabling Spying	A September 2023 article on the English-language website of the *China News Service* reported on the PRC's Ministry of State Security's (MSS) revelation of U.S. infiltration of Huawei via the NSA's Tailored Access Operations (TAO) dating back to 2009. The MSS claimed TAO carried out thousands of attacks targeting the PRC, stealing extensive high-value data.[8] This release countered U.S. and other government outcries against Huawei as a state enabler of PRC cyber operations.
Targeting Education	In September 2023, both the *South China Morning Post* and the *Global Times* published articles identifying the NSA of cyber surveillance and data theft against Northwestern Polytechnical University, claiming a PRC team found "thousands of network devices" infected by NSA spyware.[9]
High-Value Targets	In August 2023, the *Global Times* reported a joint public-private investigation that revealed U.S. cyber military team cyber espionage attacks against the Wuhan Earthquake Monitoring Center, which monitors earthquake activity. Per a leading Chinese cybersecurity company's analysis, the attacks sought to steal geological data to better understand battlefield terrain.
Global Surveillance	In February 2022, Chinese cybersecurity company Pangu Lab identified that for more than a decade the NSA had conducted global surveillance against 45 countries and regions. This marked the first time a Chinese company publicly shared technical evidence of a state-orchestrated cyber attack by alleged U.S. cyber actors.[12] It also strongly suggested that the U.S. was the world's most prominent cyber threat actor conducting global surveillance against friendly and adversarial nations alike. Several Chinese media sources echoed a report by a cybersecurity company in Burma that detailed TAO efforts to remotely obtain more than 97 billion Internet data records along with 124 billion phone records in 30 days.[13] While never made publicly available, references to this report casts the U.S. as a global spying and cyber thief.

Table 1. Cyber Themes Highlighted in Chinese Media Campaigns.

The PRC's assertive campaign benefits from the fact that governments need not prove attribution so much as to simply claim a government is responsible for a cyber attack. Unlike conventional crimes like terrorism or nuclear arms development, governments may be hesitant to "show their work" when it comes to cyber attack attribution, which can compromise sensitive collection platforms and mechanisms. This may be one of the reasons why cyber security companies actively produce APT reports and are more willing to attribute activity to a nation state, and certainly calls into question if these companies are collaborating or at least taking

direction from their host governments. Among leading cybersecurity companies, Kaspersky is one of the few that avoids attributing cyber attacks to specific governments, instead preferring the more generic classification of "state actor." As Eugene Kaspersky said in an interview, "we never do attribution."[14]

Under Xi, the PRC adopts a more aggressive stance as to its position in the world and it combats negative perceptions that it is a nefarious cyber actor. The PRC no doubt views Washington's constant harassment of its cyber activities as hypocritical, and counters with calling out the U.S. for similar activities. What has undoubtedly helped fuel the PRC's message are the Edward Snowden leaks and the Shadow Brokers, a murky group that reinforced suspicions that the U.S. cyberspace mischief exceeds that of the PRC. The 2013 Snowden treasure trove revealed highly sensitive U.S. technologies and exposed the expanse and breadth of U.S. surveillance capabilities. Many already suspected the U.S.'s formidable resources; the Snowden leaks removed all doubt. Documentaries such as *CitizenFour* and films like *Snowden* kept the image of the U.S. as a global surveillance ogre, and augmented the PRC's campaign to chip away at the U.S. image as a democratic champion and frame us more as a cyber hegemon protecting our superiority in cyberspace, superiority that has steadily declined as more governments embraced and implemented technology to support their own national interests.

The U.S. had not yet recovered from the Snowden disclosures when the mysterious Shadow Brokers group leaked the tools allegedly used by the NSA, exposing tools and vulnerabilities used to break into routers, platforms like Microsoft Windows, Linux mail servers, and even the SWIFT banking network.[15] While no definitive proof tied this group to the NSA, in early 2017 a former NSA contractor was arrested for stealing 75% of TAO's hacking tools, strengthening the assumption that the Shadow Brokers included at least one ex-NSA operative.[16] After the 2017 incident, the Shadow Brokers never resurfaced. The leak was very likely intended to embarrass the U.S. and otherwise thwart future activities. More damning, any doubt about U.S. global spying was removed. Washington could no longer deny its formidable spying endeavors, and now friendly nations like France[17] and Germany[18] were protesting against the U.S. for doing the same thing against them. For the leading democratic nation, such activities beyond the guise of "national security" are difficult to spin.

For most of 2023, the Chinese press has pushed the "U.S. cyber hegemon" narrative, which also conincided with PRC's perception of U.S. weakness on the global stage. *The Global Times*, *China Military,* and *China Daily* and PRC-allied news sources like Iran's *Tasnim News Agency*,[19] ran articles in 2023 condemning the U.S. as a cyber hegemon bully, which was imperiling rather than strengthening for global security. The articles reported continued development of U.S. cyber military apparatus, to include deployed hunt-forward teams, CIA's hacking activities, and U.S. reluctance for embracing multilateral Internet governance.[20]

Another PRC accusation is the U.S.'s willingness to levy cyber sanctions in coercing the global community. The *Global Times* reported the U.S. sanctions and places companies on export

control lists to protect its military and cyber hegemony under pretence of national security, obfuscating its true purpose – to thwart PRC competition and growth.[21] Supporting reasons for such sanctions included "human rights violations" and "invasion of privacy" concerns – two subjects the PRC would counter in subsequent press articles by showing where the U.S. was guilty of the very same allegations. The PRC is fervently committed to highlighting hypocracies and otherwise tarnishing the U.S.'s reputation as a beacon of democratic principles.

This has been facilitated by the political polarization in the U.S., particularly as to state-orchestrated surveillance, a charge frequently levied against the PRC and other authoritarian regimes by Western governments. Indeed, even organizations such as the American Civil Liberties Union acknowledges rampant overreach by surveillance authorities, particularly from the NSA.[22] Capitalizing on internal U.S. controversies, the *Global Times* quickly spearheaded a campaign to show hypocritical policies the U.S. has engaged in with its own citizens, depicting a surveillance state driven by FBI, CIA, and even Immigration and Customs Enforcement,[23] thereby exposing U.S. hypocrisy, especially over human rights issues.[24]

THE PRC'S "FREE" MEDIA AGAINST THE U.S.

Throughout Xi's tenure, and especially over the past eighteen months, the PRC has become increasingly combative toward critics that singled out the PRC for cyber offenses. The PRC has ramped up efforts to smear the U.S. not just from a cyber perspective, but in other areas as well, as evidenced by its media voraciously publishing negative news about the U.S. (and other Western governments that threaten the PRC) on topics that include poverty, pollution, oligarch control of politics, and racial tensions.[25] The increasing tempo of this negative press prompted the U.S. Department of State to report on the PRC's broader disinformation campaigns designed to shape the global information environment to favor PRC interests,[26] noting these campaigns include propaganda, censorship, promoting digital authoritarianism, and exploiting international partnerships, in short, tactics the Chinese press claim against the U.S.[27]

What is certainly noticeable is the PRC's shift in posture with respect to how it's been pursuing its goals, moving from passive "peaceful development" under Hu Jintao to a more aggressive and ambitious "national rejuvenation" strategy role under Xi's stewardship.[28] A critical part of this shift has been the PRC's willingness to go after its detractors and critics that seek to hurt the PRC's image or impede their global social, cultural, and economic gains. It also has required the PRC to take advantage of situations where their principal adversary – the U.S. – has been at its weakest. Over the past several years, the U.S. has steadily declined as an international presence, in part due to internal (border issues, race and gender issues, etc.) and external crises (Ukraine war, Israel-Palestine conflict), which have stretched its standing and, to a certain extent, its capabilities.[29]

The PRC flags key issues in an attempt to cast the U.S. as a "flawed democracy." Indeed, the 2022 *Democracy Index* report by the Economic Intelligence Unit found that the U.S. ranked

26th of 167 countries when measuring elections, government, and civil liberties, among other categories.[30] Unsurprisingly, this has been a theme in the PRC's government communications and one the Chinese media has contributed to significantly, exploiting those issues where the U.S. has been traditionally strong, (e.g., human rights, standing by its word on the global stage, etc.) to create fissures in the U.S.'s image as the leader of the free world, a position it unofficially has enjoyed since the Cold War.[31] Four recent issues that underscore the PRC's discrediting efforts include the botched Afghan withdrawal; perceptions of U.S. censorship of social media; perceptions of targeting political opponents; and allegations of U.S. spying.

Themes	Chinese Media "Naming and Shaming" Campaigns
Afghan Withdrawal	Though most Americans favored te U.S. withdrawl from Afghanistan, the hasty manner in which it occurred[32] was perceived in the European press as a U.S. failing,[33] leaving Americans behind, resulting in the death of 13 U.S. Marines and reportedly failing to consult or coordinate with allies.[34] In short, it was viewed as a blunder by both domestic and international audiences alike, as corroborated by a Department of State report released in 2023.[35] PRC media exploited this to cast the U.S.as an unreliable partner and one that will put its own interests first despite its asserted commitments in an obvious effort to convince Taiwan to not rely on U.S. help as tweeted bythe *Global Time*s editor on social media.[36]
U.S. Censorship of Social Media	The PRC also exploited reported instances of U.S. government pressuring social media companies to censor and/or restrict to the U.S. public, including COVID-related issues and the Hunter Biden laptop, citing a lawsuit accusing the U.S. government of unconstitutional censorship.[37] Despite the fact that the U.S. Supreme Court sided with the Adminsistation, first on an interim basis in September 2023, and ultimately in a 6-3 final decision in June of 2024, this did not prevent the PRC media from trying to exploit U.S. policy regarding authoritarian surveillance and censorship, claiming it to be hypocritical, and running news articles calling the U.S. a "surveillance empire" and an "empire of lies."[38]
Targeting Political Opponents	U.S. politics, according to some factions, is increasingly strained. When government agencies take actions against members of the opposing political party, it is reminiscient of authoritarian regimes that seek to remain in power. Indeed, Mike Pompeo, Secretary of State in the Trump Administration in 2022 went so far as to accuse the Biden Administration of leveraging government agencies like the FBI and Department of Justice against a political rival in the upcoming 2024 U.S. presidential election.[39] A March 2023 poll found that nearly two-thirds of those responding thought the FBI had become politically weaponized.[40] This was not the first time an Administration was accused of such an abuse of power. In 2017, the Internal Revenue Service was accused of delaying approvals of nonprofit status for conservative groups engaged in public education and voter mobilization.[41] For each of these instances, the Chinese press has feverishly seized the narrative[42] in the PRC's effort to accentuate U.S. hypocrisy and deem the U.S.'s "politics of retaliation" as counter to the even-handed principles of democratic governance.[43]
U.S. Spying	*The Global Times*, exploiting a *Wall Street Journal* (WSJ) article that detailed the CIA's spying activities against the PRC, charged the U.S. with hypocrisy when we accuse the PRC of its relentless spying.[44] The WSJ article recounted a CIA spying failure a decade ago in the PRC when U.S. spies allegedly were caught, thereby setting back U.S. intelligence work.[45] The *Japan Times* reported the CIA as having doubled its spending against the PRC and increased its own surveillance against Chinese companies.[46] This article also reported the CIA as investing heavily into intelligence collection on Chinese companies developing advanced technologies like Artificial Intelligence, information the U.S. had not typically collected in the past.[47] From this, the PRC crafted narratives to promote its own anti-espionage activities as dealing costly blows to U.S. spy agencies efforts while claiming the gap between our two intelligence services has greatly narrowed.[48]

Table 2. Geopolitical Themes Highlighted in PRC Media Campaigns.

IS CHINA'S MEDIA CAMPAIGN WORKING?

Media attacks against U.S. cyber policies complement the PRC's overall efforts to enhance perceptions of U.S. weakness and untrustworthiness and further tarnish the U.S. brand. And while we cannot accurately correlate Chinese media themes' and actual global perceptions of the U.S., the PRC's media campaigns are very real, as are these perceptions. Two prominent

polling organizations found that the U.S. has lost credibility over the past few years both internally and externally. In 2022, a Gallup poll found that the U.S. earned the least confidence from its citizens of any G7 member country besides the United Kingdom, falling to 40% in 2021 and 31% in 2022.[49] Pew Research found that of 24 countries surveyed (mostly Western), the majority found the U.S. better than the PRC, however, they also overwhelmingly believed that the U.S. constantly interfered in other countries' affairs.[50] The same survey also confirmed positive views of the U.S. as compared to the PRC in terms of military strength, entertainment, high education, standards of living, and personal freedoms but noted on economics and technology, the PRC and the U.S. drew nearly even, suggesting areas that the PRC could strengthen its engagement with international partners. It would not be surprising to see Beijing increase its efforts in these areas over the next twelve months in an effort to gain competitive advantage over the U.S.

Still, despite the PRC's prolific production of content, the Department of State report correctly concluded that PRC-driven information campaigns have yielded mixed results, which is supported by the two surveys cited above, and many in the global community still favor the U.S. over the PRC. Yet, governments need not like or agree with a country to do business with it. Case and point: the first 11 months of 2023 saw PRC exports of USD $458.5 billion to the European Union, while corresponding imports totalled USD $357.8 billion.[51] Thus, even with the majority of European states not liking the PRC's policies, a European Council on Foreign Relations reported that most of the continent views the PRC as a "necessary trade partner" and not an adversary.[52] And Europe is not alone, the PRC is the top trading partner for more than 120 countries, to include developing nations in Latin America, Africa, and Asia.[53]

This economic reality matters in framing the PRC's strategic priorities like Taiwan, and some EU countries may well recuse themselves from a cross-strait conflict or provide little substantive aid to Taiwan. The PRC does not need Europe as a military ally as much as it needs Europe to embrace economic advantage over a geopolitical incident that little impacts their continent, and also to avoid overtures to form coalitions against the PRC's interests. And French President Macron, in an April 2023 visit to the PRC, urged Europe to reduce dependence on the U.S., saying that France should not take its cues from the U.S. on issues like Taiwan and be dragged into such unnecessary conflicts.[54]

And this may very well be the crux of the PRC's media attacks. By steadily trying to chip away at the U.S.'s credibility, tarnishing our image as a democratic paragon, and exposing hypocrisies, the PRC may be more focused on sidelining foreign governments rather than creating new allies. It only needs to instill enough doubt about the U.S. to weaken resolve, soften stances, and otherwise avoid governmental barriers on issues the PRC deems vital to its interests such as Taiwan, becoming the world's largest economy, and being a leader and integrator of emerging technologies. Uncoincidentally, their media attacks against the U.S. on cyber-related matters ties directly to each of these core objectives.

CONCLUSION

The U.S. Department of State's report confirms the PRC's efforts to shape the global information environment appear less about spinning a faulty narrative than capitalizing on, even exaggerating, existing discord and distrust. But to claim the PRC is fabricating discord is conspiciously disingenuous and thus, not even credible. That the PRC's campaigns have become increasingly voluminous and pervasive strongly suggests that the PRC perceives the U.S. as vulnerable on the world stage.

The PRC's media attacks bend more toward influence than incitement, suggesting a PRC nuanced objective. The themes are consistent regardless of the topic and center on one theme – the U.S. is no longer essential in today's geopolitical environment, or anywhere near as essential as it was in the past, going back to World War II. The U.S. no longer embraces the same democratic principles it once championed, is increasingly guilty of demanding "do as I say, not as I do," and has an increasingly tarnished public image. At World War II's end, the U.S.'s role internationally was one of global leadership, fueled by the world's strongest economy and a built-up military.[55] But in the past 20 years, the U.S. gradually retreated from that position due to a failure to take decisive action or otherwise achieve U.S. policy goals responsive to international incidents, with some leaders blaming one or another administration.[56]

Fast forward to today, and it's apparent that the United States has continued this trend, suffering several foreign policy missteps and inconsistencies, especially with the two largest elephants in the room (Ukraine war, Palestine conflict) and the disparity in the support the U.S. has provided Ukraine and Israel. This is disconcerting given that in an October 2023 speech, President Biden directly linked both of their outcomes to the security of the U.S.[57] Adding insult to injury are the governments of Saudi Arabia, China, and Iran blatantly disrespecting the U.S. on the global stage by ignoring U.S. overtures for executive-to-executive engagement over oil production, stalling on restarting military-to-military communication, or using returned millions in frozen funds without restriction.[58] This further perpetuates the image that the U.S.'s influence may not be as what it once was.

Chinese media attacks against the U.S. on cyber-related issues have potential greater ramifications than just solely discrediting our government. The global community has failed to make any significant progress on codifying cyber norms of state behavior in cyberspace as well as other key areas like state cyber sovereignty. Viewed from this perspective, this Chinese media campaign can be seen as a vehicle to influence those governments in the United Nations to align themselves with either the PRC or Russian preference for a government-led approach to Internet governance as opposed to the West's multi-stakeholder model.[59] At best, the PRC gains support in the UN. At worst, continued failure to agree to a consensus perpetuates the status quo where nation states continue to act with impunity in cyberspace with minimal repercussion.

What seems clear from what is not classified is that the U.S. has not exercised a strong strategy against the PRC's cyber malfeasances, which suggests greater concern for the potential benefits of a relationship and avoiding conflict. Washington must endeavor to maintain a productive working relationship, even as the two remain fierce competitors and borderline adversaries. And the PRC understands that its active cyber apparatus notwithstanding, it cannot match the U.S. in capability, sophistication, and reach. So, instead of meeting it head on, it will leverage demonstrations of U.S. cyber power to buttress assertions that Washington's cyber program overreaches with its hunt-forward operations and overly aggressive in efforts to govern the Internet.

Xi's current strategy with the media campaign does not appear to seek to supplant the U.S. as the reigning global cyber power, but rather, to keep it in check. It does that best by publicizing its cyber activities against the PRC to depict the U.S. as an irresponsible state cyber actor. The strategy may or may not succeed and may be better observed in the UN as Internet governance issues play out. As the Department of State report confirms, the PRC's focus is more on influencing the greater information space, and less on showing it has bigger cyber muscles than Washington. Because true power comes not from disrupting or destroying infrastructures but by setting the standards and norms in the domain where such battles are and will be fought.

DISCLAIMER

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the U.S. Government.

NOTES

1. For more on China's disinformation campaign to influence our elections and amplify divisive U.S. political issues see: Jeremy B. Merrill, Aaron Schaffer, and Naomi Nix, "A Firehouse of Antisemitic Disinformation from China Pointing at Two Republication Legislators," (October 10, 2024). *The Washington Post*, https://www.washingtonpost.com/technology/2024/10/10/us-elections-china-influence-x/.
2. Jim Randle, "China Says it Is Victim of Cyber Attacks; Not Victim," (March 19, 2013). *Voice of America News*, www.voanews.com/a/china-says-it-is-victim-of-cyberattacks-not-perpetrator/1624718.html; A Martinez and Emily Feng, "China Denies Cyberattack Accusations; And Says It Too Is A Victim of Hacking," (July 20, 2021). *NPR*, https://www.npr.org/2021/07/20/1018271511/china-denies-cyberattack-accusations-and-says-it-too-is-a-victim-of-hacking.
3. Dustin Waltz and Josh Chin, "U.S. Believes It Doesn't Need to Show Proof Huawei is a Spy Threat," (January 23, 2009). *The Wall Street Journal*, https://www.wsj.com/articles/u-s-believes-it-doesnt-need-to-show-proof-huawei-is-a-spy-threat-11548288297.
4. Qihoo 360, "APT-C-39," (March 2020), http://blogs.360.cn/post/APT-C-39_CIA_EN.html; Pierluigi Paganini "CIA Hacking Unit APT-C-39 Hit China Since 2008," (March 2020). *Security Affairs*, https://securityaffairs.co/98885/apt/cia-hacking-china.html.
5. *The Global Times*, "Foreign Spy Conducts Cyberattacks Against China's Defense, High-Tech Firm by Recruiting Chinese Developer," (November 27, 2023). https://www.globaltimes.cn/page/202311/1302547.shtml.
6. *The Global Times*, "Cyber Governance Should Not Be Controlled by Group Politics, Zero Sum Thinking," (November 8, 2023). https://www.globaltimes.cn/page/202311/1301441.shtml.
7. *The Global Times*, "Playing 'A Thief Crying Stop Thief' Trick, U.S. Only Wants Permanent Cyber Hegemony," (September 20, 2023). https://www.globaltimes.cn/page/202309/1298564.shtml.
8. Li Yan, ed., "China's Ministry of State Security Reveals U.S. infiltration of Huawei Traced Back to 2009," (September 20, 2023). Ecns.cn, http://ecns.cn/news/politics/2023-09-20/detail-ihctfqzx3360335.shtml.
9. William Zheng, "Beijing Says It Uncovered US National Security Agency Operatives Behind Cyberattack on Chinese University," (September 14, 2023). *SCMP.com*, https://www.scmp.com/news/china/politics/article/3234492/beijing-says-it-uncovered-us-national-security-agency-operatives-behind-cyberattack-chinese; Yuan Hong, "Identity of NSA Hacker Behind Cyberattack on China's Leading Aviation University Identified; to Be Disclosed in Due Course: Source," (September 14, 2023). *The Global Times*, https://www.globaltimes.cn/page/202309/1298164.shtml.
10. Yuan Hong, "Exclusive: China Identifies the Culprits Behind Cyberattack on Wuhan Earthquake Monitoring Center, A Secretive U.S. Global Reconnaissance System to Be Exposed," (August 14. 2023). *The Global Times*, https://www.globaltimes.cn/page/202308/1296226.shtml.
11. Yuan Hong, "Exclusive: Hackers Behind Cyberattack on Wuhan Earthquake Monitoring Center Aims at Stealing Geological Data: Top Cybersecurity Expert," (August 2, 2023). *The Global Times*, https://www.globaltimes.cn/page/202308/1295511.shtml.
12. Cao Siqi, "Exclusive: Evidence of U.S. Monitoring 45 Countries, Regions Exposed by Chinese Security Experts for the First Time," (February 23, 2022). *The Global Times*, https://www.globaltimes.cn/page/202202/1252952.shtml.
13. Qian Gong, "U.S.: Top Threat to Global Security," (September 22, 2022). *STDaily.com*, Google Translation to English, https://www.stdaily.com/English/BusinessNews/202209/c5f6006a75d0461la8e0f187f0cc8946.shtml; *China Daily*, "U.S. Hackers Extend Malicious Cyber Operations Around the World," (July 1, 2022). https://global.chinadaily.com.cn/a/202207/01/WS62be9236a310fd2b29e69d8c.html; *China Global Television Network (CGTN)*, "Operation Black Hand: U.S. Is the Primary Threat to Global Cyber Security,"(June 16, 2022). *CGTN.com,* https://news.cgtn.com/news/2022-06-16/Operation-Black-Hand-U-S-the-primary-threat-to-global-cyber-security-1aAC9I6xDu8/index.html.
14. BN Americas, "Eugene Kaspersky: 'We work with governments, not for them,' " (November 7, 2018). *BN Americas*, Chile', Interview with Eugene Kaspersky, https://www.bnamericas.com/en/interviews/eugene-kaspersky-we-work-with-governments-not-for-them--.
15. Bruce Schneier, "Who Are the Shadow Brokers?" (May 23, 2017). *The Atlantic*, https:// www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/.
16. Dan Goodin, "Former NSA Contractor May Have Stolen 75% of TAO's Elite Hacking Tools," (February 6, 2017). *Ars Technic*a, https://arstechnica.com/tech-policy/2017/02/former-nsa-contractor-may-have-stolen-75-of-taos-elite-hacking-tools/.

NOTES

17. John Irish and Elizabeth Pineau, "Obama Reassures France After 'Unacceptable' NSA Spying," (June 24, 2017). *Reuters*, https://www.reuters.com/article/us-france-wikileaks-idUSKBN0P32EM20150623/.
18. *Reuters*, "U.S. Spied on Merkel and Other Europeans Through Danish Cables – Broadcaster DR," (May 31, 2021). *Reuters*, Copenhagen, https://www.reuters.com/world/europe/us-security-agency-spied-merkel-other-top-european-officials-through-danish-2021-05-30/.
19. *Tasnim New Agency,* "China Says US Seeks Cyber Hegemony," (April 8, 2023). *Tasnim News Agency*, Tehran, https://www.tasnimnews.com/en/news/2023/04/08/2877120/china-says-us-seeks-cyber-hegemony
20. Wang Qiang, "U.S. Eager to Seek Cyber Military Hegemony," (May 5, 2023). *China Military,* http://eng.chinamil.com.cn/OPINIONS_209196/Opinions_209197/16222055.html; Zhou Ningan, "Hacking Empire's Cyberspace Hegemony Endangers Global Security," (May 9, 2023). *China Military*, http://eng.chinamil.com.cn/WORLD_209198/WorldMilitaryAnalysis/16223609.html; *China Daily*, "Cyberspace Shouldn't Be a New Battlefield," (July 25, 2023). https://www.chinadaily.com.cn/a/202307/25/WS64bfb5b2a31035260b8186d2.html; Zhou Jin, "Beijing Speaks Out Against U.S.' Cyber Deployments," (August 10, 2023). *China Daily,* https://www.chinadaily.com.cn/a/202308/10/WS64d4ed9da31035260b818b6c3.html.
21. Global Times Staff Reporters, "Bullying Empire: How the U.S. Tries to Rule World's Internet Through Sanctions, China Slander Campaigns," (June 15, 2023). *The Global Times*, https://www.globaltimes.cn/page/202306/1292661.shtml.
22. Sarah Taitz, "Five Things to Know about NSA Mass Surveillance and the Coming Fight in Congress," (April 11, 2023). *American Civil Liberties Union*, https://www.aclu.org/news/national-security/five-things-to-know-about-nsa-mass-surveillance-and-the-coming-fight-in-congress.
23. Xin Ping, "Life in the U.S. 'Empire of Surveillance': Trapped in a Dragnet," (August 12, 2022). *The Global Times*, https://www.globaltimes.cn/page/202208/1272851.shtml.
24. Tang Lan, "Surveillance Empire: Unrestricted Eavesdropping on Allies, Citizens Exposes Hypocrisy of American Human Rights," (May 25, 2023). *The Global Times*, https://www.globaltimes.cn/page/202305/1291394.shtml.
25. Hwang Chun-mei and Gu Ting for RFA Mandarin, "Chinese State Media is Pumping Out Bad News About U.S., Britain," (July 16, 2023). *Radio Free Asia*, https://www.rfa.org/english/news/china/china-bad-news-07112023142511.html.
26. United States Department of State, "How the People's Republic of China Seeks to Reshape the Global Information Environment," (September 28, 2023). Global Engagement Center Special Report, //www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/.
27. The People's Republic of China Ministry of Foreign Affairs, "Foreign Ministry Spokesperson's Remarks on the U.S. State Department's Report Targeting China," (September 30, 2023). *Ministry of Foreign Affairs*, https://www.mfa.gov.cn/eng/xwfw_665399/s2510_665401/2535_665405/202309/t20230930_11154141.html.
28. The People's Republic of China, "China's Peaceful Development,"(September 2011). Government of PRC, https://english.www.gov.cn/archive/white_paper/2014/09/09/content_281474986284646.htm; Xi Jinping, "Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era," (October 18, 2017). Remarks, Chinese Communist Party Conference, http://xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.
29. Kathryn Levantovscaia, "Overstretched and Undersupplied: Can the US Afford its Global Security Blanket?" (January 5, 2024). *The Atlantic Council*, https://www.atlanticcouncil.org/blogs/new-atlanticist/overstretched-and-undersupplied-can-the-us-afford-its-global-security-blanket/; *Time Magazine Online*, "Is the U.S. Military Stretched Too Thin?"(original post August 23, 2003). Blog. https://content.time.com/time/nation/article/0,8599,477917,00.html
30. David Myers, "U.S. Remains a Flawed Democracy in Annual Rankings," (February 14, 2022). *The Fulcrum*, https://thefulcrum.us/big-picture/Leveraging-big-ideas/flawed-democracy.
31. *Encyclopedia of American Foreign Relations*, "Exceptionalism: The Leader of the Free World," (accessed May 1, 2024). https://www.americanforeignrelations.com/E-N/Exceptionalism-The-leader-of-the-free-world.html.
32. *United States Department of State,* "After Action Review of Afghanistan: January 2020-August 2021,"(March 2022), Report, https://www.state.gov/wp-content/uploads/2023/06/State-AAR-AFG.pdf.
33. "Allies Round on US After Afghanistan Withdrawal," (August 16, 2021). *France24 News Online*, https://www.france24.com/en/live-news/20210816-allies-round-on-us-over-afghanistan-debacle.
34. "Allies Round on US After Afghanistan Withdrawal."
35. *United States Department of State*, "After Action Review of Afghanistan: January 2020-August 2021,"(March 2022), Report, https://www.state.gov/wp-content/uploads/2023/06/State-AAR-AFG.pdf.

NOTES

36. Hu Xijin, *Global Times Editor*, China: Twitter Account Post, (August 16, 2021). https://twitter.com/HuXijin_GT/status/1427268690835705860.
37. Gabe Kaminsky, "Top Republicans Throw Support Behind Major Biden Censorship Lawsuit by Conservative Media," (December 11, 2023). *Washington Examiner*, https://www.washingtonexaminer.com/news/house/republicans-support-biden-censorship-lawsuit-gdi-newsguard.
38. Tang Lan, "Surveillance Empire: Unrestricted Eavesdropping on Allies, Citizens Exposes Hypocrisy of American Human Rights," (May 25, 2023). China: *The Global Times*, https://www.globaltimes.cn/page/202305/1291394.shtml; *China Daily*, "U.S. Attempts to Deceive World With Its Empire of Lies," (March 31, 2022), https://global.chinadaily.com.cn/a/202203/31/WS6244fc67a310fd2b29e5446b.html.
39. Michael R. Pompeo, "FBI Weaponized by Biden Justice Department in Campaign Against Trump," (August 12, 2022). *Fox News*, https://www.foxnews.com/opinion/fbi-weaponized-biden-justice-department-campaign-trump.
40. Anugrah Kumar, "Nearly Two Thirds of Voters Think FBI Has Been Politically Weaponized, Poll Suggests," (March 13, 2023). *Congresswoman Harriet Hageman's Website*, https://hageman.house.gov/media/in-the-news/nearly-two-thirds-voters-think-fbi-has-been-politically-weaponized-poll-suggests.
41. Bradley A. Smith, "A Lesson on the Abuse of Power By Obama and His Senate Allies," (October 10, 2017). *The Hill*, https://thehill.com/opinion/white-house/354680-a-lesson-on-abuse-of-power-by-obama-and-his-senate-allies/.
42. Jeremy B. Merrill, et. al., "A Firehouse of Antisemitic Disinformation from China Pointing at Two Republication Legislators."
43. Global Times Staff Reproters, "U.S. Falls Further into 'Politics of Retaliation' Amid Biden's Garage-Gate," (January 13, 2023). China: *The Global Times*, https://www.globaltimes.cn/page/202301/1283783.shtml.
44. Global Times, "Why is the CIA Openly Discussing Its Misdeeds Against China?" (December 27, 2023). Editorial, China: *The Global Times*, https:// www.globaltimes.cn/page/202312/1304439.shtml.
45. Warren P. Strobel, "American Spies Confront a New, Formidable China," (December 26, 2023). *The Wall Street Journal*, https://www.wsj.com/politics/national-security/american-spies-confront-a-new-formidable-china-5c384370.
46. Edward Wong, Julian E. Barnes, Muyi Xiao, and Chris Buckley, "Chinese Spy Agency Rising to Challenge the CIA," (December 28, 2023). *The Japan Times*, https://www.japantimes.co.jp/news/2023/12/28/asia-pacific/politics/chinese-spy-agency-cia/.
47. Wong, et al., "Chinese Spy Agency Rising to Challenge the CIA."
48. Yang Sheng and Zhang Yuying, "Anti-Espionage Efforts of China Against U.S. Spies 'Essential, Effective,' " (December 27, 2023), China: *The Global Times*, https://www.globaltimes.cn/page/202312/1304440.shtml.
49. Benedict Vigers, "Confidence in U.S., UK Governments Lowest in G," (July 3, 2023). *Gallup*, https://news.gallup.com/opinion/gallup/507950/confidence-governments-lowest.aspx.
50. Laura Silver, Christine Huang, Laura Clancy, Nam Lam, Shannon Greenwood, John Carlo Mandapat, and Chris Baranovski, "Comparing Views of the U.S. and China in 24 Countries," (November 6, 2023). *Pew Research*, https://www.pewresearch.org/global/2023/11/06/comparing-views-of-the-us-and-china-in-24-countries/
51. Zen Soo, "China's Exports in November Edged Higher for the First Time in 7 Months, While Imports Fell," (December 7, 2023). *AP News*, https://apnews.com/article/china-exports-imports-decline-economy-7eabaf75c502f943afdd122e12b26dc.
52. Jana Puglierin and Pawel Zerka, "Keeping America Close, Russia Down, and China Far Away," (June 7, 2023). *European Council on Foreign Relations*, https://ecfr.eu/publication/keeping-america-close-russia-down-and-china-far-away-how-europeans-navigate-a-competitive-world/.
53. Ambassador Mark A. Green, "China is the Top Trading Partner to More Than 120 Countries," (January 17, 2023). *Wilson Center*, https://www.wilsoncenter.org/blog-post/china-top-trading-partner-more-120-countries; Igor Patrick, "China's Latin American Investments Downshift to Smaller, More Strategic Projects," (February 22, 2024). *SCMP News*, https://www.scmp.com/news/china/article/3252865/chinas-latin-american-investments-downshift-smaller-more-strategic-projects; Marcus Vinicius de Freitas, "The Impact of Chinese Investments in Africa: Neocolonialism or Cooperation?´(August 2023), *Policy Center for the New South (PCNS)*, Morocco, https://www.policycenter.ma/sites/default/files/2023-08/PB_30-23_Marcus%20Freitas.pdf; and Cissy Zhou, "Chinese Investment in Asia Rose 37% in 2023, Led by Indonesia," (March 7, 2024). *Nikkei Asia*, https://asia.nikkei.com/Spotlight/Belt-and-Road/Chinese-investment-in-Asia-rose-37-in-2023-led-by-Indonesia.

NOTES

54. Michael Shurkin, "Macon in Beijing: Why U.S.-China Watchers Need to Take a Deep Breath," (April 13, 2023). *The Hill*, https://thehill.com/opinion/international/3948006-macron-in-beijing-why-us-china-watchers-need-to-take-a-deep-breath/.
55. Jared Cohen, "The Global Credibility Gap," (December 6, 2023). *Foreign Policy*, https://foreignpolicy.com/2023/12/06/global-geopolitics-credibility-us-china-competition-alliances-deterrence-military-economic-power/.
56. *Congressional Research Service*, "U.S. Role in the World," (April 6, 2020), https://crsreports.congress.gov/product/pdf/R/R44891/47.
57. Myah Ward and Jonathan Lemire, "Biden: America at an Inflection Point in Israel and Ukraine," (October 19, 2023). *Politico*, https://www.politico.com/news/2023/10/19/biden-terrorist-must-pay-a-price-for-their-terror-00122644.
58. Edward Helmore, "Saudi Arabia and UAE Leaders 'Decline Calls With Biden' Amid Fears of Oil Price Spike," (March 8, 2022). *The Guardian*, https://www.theguardian.com/us-news/2022/mar/09/saudi-arabia-and-uae-leaders-decline-calls-with-biden-amid-fears-of-oil-price-spike; *Reuters,* "U.S. In Touch With Beijing About Arranging Military Communication," (December 12, 2023). https://www.reuters.com/world/us-touch-with-beijing-about-arranging-military-communication-pentagon-2023-12-12/; Sabrina Martin, "Iran Humiliates Joe Biden: Will Use Unfrozen Money As It Pleases," (September 13, 2023). *Vox*, https://voz.us/iran-humiliates-joe-biden-will-use-unfrozen-us-money-as-it-pleases/?lang=en.
59. Shane Tews, "China Challenges Multi-Stakeholder Model of Internet Governance," (December 23, 2015). *AEI*, https://www.aei.org/technology-and-innovation/china-challenges-multi-stakeholder-model-internet-governance/.

GenAI in the 2024 Taiwan Presidential Election: Lessons for Democracies

Major Sarah Mobilio, USMC

ABSTRACT

This article examines the use of generative artificial intelligence (GenAI) in disinformation campaigns during the 2024 Taiwan presidential election, with a focus on the People's Republic of China's (PRC) tactics and Taiwan's countermeasures. PRC state and non-state actors utilized GenAI to produce subtle and less detectable disinformation, including deepfakes and biased language models. Taiwan's curated response to PRC-affiliated information threats feature legislative actions, media literacy initiatives, and development of its own GenAI tools, such as the Trustworthy AI Dialogue Engine (TAIDE) language model, to safeguard its cultural values. Despite the PRC's efforts, Taiwanese sentiment toward the PRC remains largely neutral or negative, demonstrating resilience in Taiwan's democratic processes. The study further explores the global implications of GenAI in disinformation campaigns, drawing parallels with Russian tactics and examining the role of U.S. technology firms in countering these threats. Taiwan's multifaceted response offers valuable insights for other democracies facing similar challenges in the evolving landscape of information warfare.

INTRODUCTION

The January 2024 Taiwan presidential election highlighted the increasing sophistication of disinformation campaigns, particularly those leveraging generative artificial intelligence (GenAI). This paper is a qualitative analysis of the 2024 Taiwan presidential election to explore how PRC state and non-state actors

Major Sarah Mobilio is a regional affairs officer and public affairs officer in the United States Marine Corps. She earned Masters' Degrees from the Naval Postgraduate School, San Diego State University, and Boston University. Her tours of duty span from North Carolina to the Pentagon, Japan, and Germany.

are employing GenAI in disinformation efforts against Taiwan and the measures Taiwan is adopting to protect its democracy.[1] GenAI is a form of machine learning (ML) that can independently learn from data patterns without human guidance.[2] Programs utilizing large language models, such as OpenAI's ChatGPT (Generative Pre-trained Transformer), represent the next evolution in text-based machine learning.[3] These models can process vast amounts of data to generate predictions and produce outputs in the form of human-like text, images, music, and code.[4]

PRC state and non-state actors have increasingly utilized GenAI to craft more subtle and less detectable disinformation. In response, Taiwan is developing its own GenAI tools, such as TAIDE, and is enhancing its detection capabilities through partnerships among technology companies, the government, and the media. Supported by legislative measures, media literacy, and international collaborations, Taiwan's proactive approach is not only helping to preserve its cultural values but also appears to be strengthening its democratic resilience. Findings suggest that despite the PRC's efforts to influence Taiwanese opinion, Taiwanese sentiment towards the PRC remains largely neutral or negative, and Taiwan's strategic use of GenAI seems to have effectively diminished the impact of PRC AI techniques.[5]

THE PRC'S USE OF GenAI IN CYBER AND DISINFORMATION CAMPAIGNS

The PRC's strategic integration of GenAI into its national and international influence efforts, as shown during the 2024 Taiwan presidential election, highlights a sophisticated approach to shaping global norms favorable to the Chinese Communist Party's (CCP) goals and values. The PRC has incorporated GenAI into its domestic censorship and content control efforts within its digital ecosystem, as part of broader effort to project power through initiatives, such as the

Belt and Road and Digital Silk Road.[6] The CCP's AI regulations, such as the July 2023 Interim Measures, enforce adherence to CCP-defined socialist values.[7] Key provisions of the Interim Measures, identified by Qiheng Chen, are content, privacy, algorithm registration, training data, fairness, and labeling.[8] Several mainstream chatbots adhering to these measures are already operational, including Baidu's Enhanced Representation through Knowledge Integration (ERNIE),[9] Alibaba's SeaLLM,[10] Hunyuan large language model (LLM)[11] in WeChat,[12] and Huawei's Pangu LLM.[13]

The PRC's GenAI advancements are not only about catching up with the U.S., but also about driving industrial productivity and economic growth. The PRC is increasingly using GenAI tools in illicit activities including cyberattacks and disinformation, which are aligned with the PRC's "Three Warfares" strategy, which has evolved into the People's Liberation Army's (PLA) concept of "cognitive domain operations" (CDO).[14] The Three Warfares strategy includes public opinion warfare, psychological warfare, and legal warfare. CDO built upon the Three Warfare's strategy to incorporate psychological, media, legal, and technological means to affect the cognitive landscape of people and populations.[15] The PRC's disinformation tactics reflect an adaptation from the Russian model of disinformation operations, which exploit vulnerabilities in democracies to sway public opinion and manage narratives.[16] Actors conducting illicit activities include state-sponsored units and independent groups who use GenAI for various cyber threats, including espionage and cyberattacks. The activities of these groups suggest a broader trend wherein state and non-state actors use GenAI in cyber operations to collect on perceived threats and project power and influence globally.[17] This includes state-sponsored cyber units, along with numerous independent non-state hacking groups and individuals.[18]

2024 PRESIDENTIAL ELECTION

Since Taiwan's first direct presidential vote in 1996, the PRC has used various tactics to influence electoral outcomes in Taiwan, with President Xi Jinping intensifying efforts through coercion, disinformation, cyberattacks, and military and diplomatic pressure to push for reunification.[19] The "U.S. skepticism" narrative, which portrays the U.S., rather than the PRC, as the primary threat to Taiwan emerged during the 2024 election, consistent with Xi's pressure.[20] The U.S. skepticism narrative was supported in the election cycle by both the Kuomintang (KMT), a main political party in Taiwan, and by Chinese-mainland state actors looking to meddle in the Taiwanese election.

The dichotomy of reunification with mainland China and the U.S. skepticism narrative is at the heart of the dynamic political environment within Taiwan. The once authoritarian KMT was the party that helped to advance the political economy of Taiwan and brought democratic elections to the island in the 1980s and 1990s. Now the KMT is seen as more amicable to China, and Taiwan's current administration, the Democratic Progressive Party

(DPP), calls for closer cooperation with other "like-minded" democracies.[21] Börjesson and Chen argue that the polarization between the DPP and KMT on China relations remains a key hurdle within Taiwan, especially in addressing foreign disinformation.[22] Without consensus, this challenge could threaten to politicize and weaken Taiwan's unified response to disinformation as well as other threats to its national security.[23]

PRC Meddling

The January 2024 Taiwanese presidential election showcased the evolving nature of PRC disinformation campaigns and marked a shift towards more sophisticated use of GenAI integration and a deeper focus on local issues and targeted attacks on the DPP.[24] The PRC followed the Soviet Union's traditional method of disinformation campaigns by planting erroneous headlines in proxy or foreign media sources.[25] The KGB's "active measures," developed in the 1980s, included front groups, targeted assassinations, forgeries, and disinformation.[26] Their contemporary disinformation model involved planting deceptive narratives in low-tier or proxy media outlets, often in foreign countries.[27] These narratives would then be reused in other countries, referencing the original source to add legitimacy.[28] The success of these campaigns depended on whether "experts" or leaders promoted the false information and if the target audience was primed to accept and share it.[29] The *Wall Street Journal* reported one of the first Chinese-generated bogus stories for the 2024 Taiwan election about a purported top-secret meeting in Taiwan where the U.S. asked Taiwan to develop bioweapons. The story gained some traction in Taiwanese media.[30] As the election drew closer, the PRC increased its use of advanced AI technologies to craft and disseminate narratives via different channels to influence the election's outcome and promote "pro-China" sentiment.[31] These advanced AI capabilities, such as targeted content optimization, automated distribution, and sentiment analysis, allowed PRC-affiliated individuals and groups to create and disseminate more convincing, targeted, and impactful disinformation campaigns.[32]

There is emerging evidence that pro-PRC actors used novel tactics, such as deepfakes, AI generated voice overs and avatars, social media chatbots, a falsified e-book and other news articles, and Chinese LLMs trained on pro-CCP party lines to meddle in the 2024 election.[33] Examples of such claims include an altered video in November 2023 that falsely portrayed Lai Ching-te, the DPP candidate, praising the party's pro-Beijing rivals.[34] Taiwanese officials quickly removed this video, deeming it an attempt to sway voters.[35] Another video critical of Lai over a railway project was posted on Douyin[36] and TikTok simultaneously, with evidence suggesting the videos originated from Douyin due to their use of simplified Chinese characters as opposed to the traditional characters used in Taiwan.[37] This Lai-railway video found a much larger audience on TikTok, receiving nearly 20 times the views it got on Douyin.[38]

Another novel PRC-affiliated disinformation tactic involved publishing a 300-page e-book titled "The Secret History of Tsai Ing-wen," which contained false allegations about Taiwan's current president. Despite the declining popularity of long-form reading, the e-book spread

on social media and email during the election period, aiming to discredit Tsai and her party, the DPP.[39] The focus on Tsai, instead of the actual candidate Lai Ching-te, possibly stemmed from her strong opposition to Beijing and was likely done with the intention to undermine Lai's candidacy by association with the salacious and scandalous falsities attributed to President Tsai.[40] This strategy is part of the PRC's broader efforts to manipulate political figures and dynamics to influence electoral outcomes as part of political warfare.[41]

The decision to make an e-book was an interesting change of tactics adapted to the GenAI age, because the book became a script for GenAI videos with social media GenAI avatars, many acting as news reporters, reading out parts of the e-book.[42] Tim Niven, a disinformation researcher in Taiwan, stated that the book itself may also have been created by GenAI.[43] Perhaps the believability of the e-book is hard to fathom. However, the more the deceptive narrative circulates within individuals' online echo chambers, the more certain predisposed groups and people become primed to believe and relay certain elements of that e-book or narrative to others, thus blurring reality.

The PRC also progressed in its attempt to influence public opinion just in the pro-PRC biased outputs from its LLMs, such as Baidu's Ernie Bot.[44] Consider an example of Ernie Bot output about the 2024 Taiwanese Presidential election:

> When asked who won the recent presidential election in Taiwan, the world's most advanced Chinese-language chatbot gives a confusing answer: "Lai Ching-te," Baidu's Ernie Bot accurately says. But then it adds: "No matter how the situation in Taiwan changes, the basic fact is that there's only one China"—a comment that echoes what Beijing's diplomats said after the U.S.-friendly candidate won the race to be the next president of the island China wants to someday rule.[45]

Ernie Bot is one of several Chinese-speaking LLMs trained on data approved by the CCP. The issue that AI researchers see in Taiwan is that AI chat bots, such as Ernie Bot, have a very strong ability to infiltrate culture.[46] In democracies such as Taiwan, technologies that promote free speech and expression largely cannot be prohibited.[47]

Lastly, PRC GenAI-enhanced disinformation tactics have enabled online actors with the ability to diversify their tactics and produce more tailored, varied, and covert communication. The 2021 RAND report by Harold, et al., underscored the PRC's enhanced capability to effectively emulate authentic Taiwanese sentiment, forecasting that AI and emerging technologies would significantly bolster the PRC's precision in cognitive warfare strategies.[48] This foresight was validated in the 2024 Taiwan presidential election when PRC-based entities deployed advanced and sophisticated tactics to micro-target specific groups, and made it challenging to trace the origins of such deceptive practices.[49] Tim Niven's analysis of social media during Taiwan's election revealed the PRC's adaptation of Russian-like strategies. He noted that some accounts switched from promoting pro-Democratic content to criticizing Taiwan in simplified Chinese (not traditional Chinese, which is predominately used in Taiwan),

similar to the operations of Russian bots and trolls.[50] Despite these efforts, the DPP won, indicating that PRC disinformation did not critically influence the election. The DPP's victory suggests Taiwanese resilience against types of disinformation and the challenges of using information warfare to affect electoral outcomes.

Taiwan Countermeasures

In response to sophisticated disinformation campaigns, Taiwan implemented a comprehensive counterstrategy that included legislative actions, enhancements in media literacy and fact-checking, and the use of GenAI to identify and neutralize misleading content. The Taiwanese government established teams within the executive branch to oversee policies for countering disinformation and to coordinate with other agencies.[51] Their efforts included promoting a framework to identify, debunk, combat, and enforce measures to reduce disinformation.[52] Pieces of legislation have been introduced, mostly prescribing penalties for spreading disinformation on specific topics that cause harm.[53] Examples of such legislation included the 2019 Anti-Infiltration Law that aimed to prohibit foreign actors from making illegal political contributions, disseminating false information, organizing campaign activities, or otherwise meddling in Taiwan's electoral processes or governmental affairs.[54] Violators of this law could face up to five years in jail and fines amounting to over $333,000.[55]

However, Taiwan faces other challenges. There is resistance from social media companies to comply with regulations and increase transparency.[56] Additionally, there is a need to find effective methodologies to evaluate the scale and impact of disinformation.[57] Lastly, measures are necessary to understand the effectiveness of punishment-based legislation.[58]

Taiwan is also adopting a more comprehensive national approach to media literacy to counter disinformation campaigns.[59] Initiated by the Ministry of Education in March 2023, the Digital Era Media Literacy Education White Paper (2023 White Paper) builds on the 2018 False Information Prevention Project.[60] It integrates "Information & Media Literacy" into the national curriculum, more formally known as the 108 Curriculum Guidelines, which serves as the foundation to Taiwan's 12-year basic education program.[61] The 2023 White Paper is an update to the 2002 framework to educate citizens across all age groups on recognizing deceptive messaging and ensuring cyber safety.[62] Highlighted by Willian Hung in his *Global Taiwan Institute* article, these 2023 initiatives aim to cultivate an informed populace capable of critical thinking, while fostering public-private collaboration and preserving media freedoms.[63]

Taiwan is now utilizing GenAI and collaborating with technology companies to identify and contextualize disinformation originating from the PRC. This collaborative approach, which combines technology with expertise, allows for a more efficient response to disinformation campaigns by automating the source and fact verification and counteracting misleading content through online and other traditional communication channels.[64] Companies such

as Ethan Tu's Taiwan AI Labs use GenAI to identify and publicize social media information manipulation.[65] Tu noted that information manipulation online during the Taiwan election became more serious and sophisticated due to the emergence of GenAI. This technology advancement enabled online troll accounts to diversify their roles, making their comments more tailored, varied, and harder to detect as being part of a coordinated campaign.[66] The use of GenAI tools helps to scale the response to disinformation and allows for faster clarification, which is crucial given the volume of deceptive content propagated by PRC-affiliated actors.

To counteract Chinese mainland LLMs, Taiwan is developing its own LLM called TAIDE, which aims to be Taiwan's first trustworthy AI application model.[67] TAIDE's research and development highlights Taiwan's civil and governmental cooperation towards advancing Taiwan's own GenAI capabilities while protecting the linguistic and cultural values inherent to Taiwan.[68] A pre-published research study from National Taiwan University assessed that the Taiwan LLM excels with traditional Chinese text and outperforms current models that are primarily trained on simplified Chinese or English.[69] But other sources mention that TAIDE's development faces challenges such as limited training data, data privacy issues, and funding.[70] Nevertheless, Taiwan's decision to create its own LLM due to the widespread availability of Chinese mainland-developed LLMs infiltrating its election and cultural norms is a new tactic to counteract disinformation in the GenAI era.[71]

Despite facing challenges inherent to democratic societies, including data privacy concerns, media freedom, the integration of media literacy, and a complex history, Taiwan is adopting a distinctive approach to counter disinformation. The government and civil society are each leveraging their strengths to foster a cooperative strategy against PRC influence in the information space. This collaborative effort highlights Taiwan's innovative experiment in how a democracy can effectively combat disinformation. It also offers valuable insights for the U.S. and other democracies on how to implement proactive measures during the priming phase of information dissemination and in non-kinetic warfare scenarios, showcasing the potential for democratic resilience in the face of global disinformation campaigns.

Other Countermeasures

Numerous U.S. technology firms are also actively countering disinformation campaigns targeting American interests, particularly those orchestrated by the PRC. In 2023, Meta, the parent company to Facebook and Instagram, identified and dismantled five adversarial networks originating from the PRC, the highest number of such actions Meta took against any country in that year.[72] These networks engaged in coordinated inauthentic behavior, or behavior to misrepresent or manipulate, to spread content that supported the PRC's narrative on human rights, criticized its detractors, and discussed the country's international rivalries, particularly with the U.S. The operations aimed to manipulate global public opinion by justifying the PRC's policies in Tibet and Xinjiang and promoting its interests in Africa

and Central Asia.[73] Despite these efforts, Meta's reports indicate that these PRC-affiliated networks have struggled to significantly influence public discourse, mainly because the operators were hindered by language differences and technological challenges.[74]

A report from Microsoft outlined how the company was staying ahead of threat actors, including those affiliated with the PRC, in the age of AI.[75] Microsoft named the threat actors and identified current ways they are using AI to collect, target, and attack individuals and groups in online environments. Microsoft found that two PRC state-affiliated cyber threat actors, Charcoal Typhoon and Salmon Typhoon, were exploring LLMs for their operations.[76] Charcoal Typhoon targeted various international sectors, using LLMs for tasks, such as reconnaissance and operational enhancement, while Salmon Typhoon focused on U.S. defense and cryptography and employed LLMs for intelligence gathering on sensitive topics and strategic interests. Both groups are in the experimental phase of integrating AI into cyber tactics.[77] In response to their activities, Microsoft disabled the Advance Persistent Threats (APTs) through advanced threat reduction and incident response (isolation and blocking), and continues to track and mitigate AI misuse in cybersecurity by enforcing multi-factor authentication and monitoring and sharing intelligence with security firms and tech corporations.[78] These actions are just a few open-source examples of the many ways in which the U.S. is actively working to eliminate online global disinformation threats from the PRC.

ANALYSIS

The precise impact that the PRC's sophisticated GenAI-enhanced influence operations have on the Taiwanese is indeterminate due to convergence of other military, economic, and diplomatic factors that impact Taiwanese attitudes and behaviors towards mainland China. However, few people in Taiwan see themselves primarily as Chinese. They identify as Taiwanese and have consistently voted for the DPP since 2002, indicating a divergence from mainland China for the past twenty-two years. In fact, it appears that the percentage of those who identify primarily as Taiwanese is slowly increasing, as the 2024 Pew Research Center survey indicated a one percent growth in "primarily Taiwanese" from its 2020 survey.[79]

Furthermore, Taiwan's dedication to countering Chinese disinformation is seemingly quite effective as its responses encompass societal education on media and digital literacy, laws to deter actors from governmental and election interference, and development of its own LLM, TAIDE, to protect Taiwan's culture, language, and institutions. TAIDE is still undergoing development, but as Jane Yung-jen Hsu, the vice chair of the government-initiated Taiwan AI Center of Excellence, stated about TAIDE,

> Frankly speaking, the resources we [the Taiwan AI Center of Excellence] are able to pour in are much less [than countries that use simplified Chinese countries]...However, what we're trying to solve are practical problems such as providing a model for those enterprises and financial institutions that are not willing to have their data provided to [models trained by non-Taiwanese groups].[80]

In other words, Taiwan is taking deliberate steps to protect its economic institutions. Building a more resilient democracy at the societal and institutional level with GenAI technology in mind is something the Taiwanese are proving very adept at, and something other democracies could study to emulate.

CONCLUSION

The PRC's sophisticated use of GenAI technologies and strategies of coercion aimed to influence the 2024 Taiwanese presidential election failed to significantly sway the outcome. This highlights the resilience of the Taiwanese and their effective employment of GenAI countermeasures. Taiwan implemented a robust blend of legislative, technological, and educational measures to safeguard its democracy against disinformation. These efforts included laws to penalize disinformation activities, technological advancements to detect and counteract deceptive messaging, and educational reforms to enhance media literacy. This collaborative approach demonstrated Taiwan's commitment to maintain its autonomy and cultural identity, making it a model for other democracies that grapple with similar threats. Future research could focus on better understanding the trustworthiness of AI technologies, gleaning better measures of effectiveness from past disinformation campaigns, and exploring how Taiwan's military approaches AI and disinformation.

DISCLAIMER

The views expressed in this work are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the United States Marine Corps, or the Department of Defense.

NOTES

1. This paper uses the terms *deceptive messaging* and *disinformation* interchangeably to encompass all different types of false or misleading information. The differences between the three types of deceptive messaging are defined here: *disinformation* is when false information is knowingly shared to cause harm; *misinformation* means the information is false, but not created or shared with the intent to cause harm; *malinformation* means that genuine information that is shared to cause harm, "often by moving information designed to stay private into the public sphere." Source: Claire Wardle and Hossein Derakhshan, "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making" (September 27, 2017), Strasbourg: Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c.
2. "What Is ChatGPT, DALL-E, and Generative AI?," (January 19, 2023). *McKinsey & Company*, https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-generative-ai.
3. "What Is ChatGPT, DALL-E, and Generative AI?"
4. "What Is ChatGPT, DALL-E, and Generative AI?"
5. Kat Devlin and Christine Huang, *In Taiwan, Views of Mainland China Mostly Negative*, (May 5, 2020). Washington, D.C.: Pew Research Center, https://www.pewresearch.org/global/2020/05/12/in-taiwan-views-of-mainland-china-mostly-negative/; Christine Huang and Kelsey Jo Starr, "Most People in Taiwan See Themselves as Primarily Taiwanese; Few Say They're Primarily Chinese," (January 16, 2024). *Pew Research Center* (blog), https://www.pewresearch.org/short-reads/2024/01/16/most-people-in-taiwan-see-themselves-as-primarily-taiwanese-few-say-theyre-primarily-chinese/; Alison Hsiao, "Taiwan-Developed Generative AI System Set to Benefit All Sectors - Focus Taiwan," (April 30, 2024). *Focus Taiwan - CNA English News*, https://focustaiwan.tw/sci-tech/202404300026.
6. Carol Lee, et al., "New Measures in Mainland China for Generative AI and Implications for Global AI Governance," (November 17, 2023). ISACA, https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/new-measures-in-mainland-china-for-generative-ai-and-implications-for-global-ai-governance; Sameer Patil and Prithvi Gupta, "The Digital Silk Road in the Indo- Pacific: Mapping China's Vision for Global Tech Expansion," *Understanding China*, Issue Brief, no. 683 (January 2024): 1–27, https://www.orfonline.org/public/uploads/posts/pdf/20240103105252.pdf.
7. Three key measures on AI regulation during this time include Internet Information Service Algorithmic Recommendation Management Provisions, Internet Information Service Deep Synthesis Management Provisions, and the Interim Measures for Generative AI. Source: Qiheng Chen, *China's Emerging Approach to Regulating General-Purpose Artificial Intelligence: Balancing Innovation and Control | Asia Society* (Asia Society Policy Institute, 2024), https://asiasociety.org/policy-institute/chinas-emerging-approach-regulating-general-purpose-artificial-intelligence-balancing-innovation-and.
8. Qiheng Chen, *China's Emerging Approach to Regulating General-Purpose Artificial Intelligence: Balancing Innovation and Control*, (February 7, 2024). Asia Society Policy Institute, https://asiasociety.org/policy-institute/chinas-emerging-approach-regulating-general-purpose-artificial-intelligence-balancing-innovation-and.
9. Baidu's ERNIE (Enhanced Representation through kNowledge Integration) is an LLM integrated into one of the Chinese internet's main search engines. Baidu created it to rival ChatGPT4. Source: Asim BN, "Baidu's Ernie 4.0 Turbo Boosts API Capacity to Handle 500 Million Queries Daily," (June 29, 2024). *Digital Information World Online*, https://www.digitalinformationworld.com/2024/06/baidus-ernie-40-turbo-boosts-api.html.
10. Alibaba's DAMO and SeaLLM are focused on research and development and multilingual capabilities to support Alibaba's e-commerce and cloud platforms throughout Asia. Source: TechNode Global Staff, "Alibaba DAMO Academy Introduces SeaLLMs, Inclusive AI Language Models for Southeast Asia," (December 11, 2023), *TNGlobal*, https://technode.global/2023/12/11/alibaba-damo-academy-introduces-seallms-inclusive-ai-language-models-for-southeast-asia/.
11. LLMs are AI systems that use transformer-based neural network structures to process and generate text. Source: "What Are Large Language Models (LLMs)?" (November 2, 2023). IBM, https://www.ibm.com/topics/large-language-models.
12. Hunyuan LLM is used in China's main social media app WeChat Source: South China Morning Post, "Tencent using Hunyuan AI model in 180 services amid competition with local rivals Baidu and Alibaba," (October 27, 2023). *Yahoo! Finance Website*, https://finance.yahoo.com/news/tencent-using-hunyuan-ai-model-093000179.html.
13. Huawei's Pangu LLM is integrated into its cloud services and consumer products across the Digital Silk Road. Source: Eric Xu, "Paving the Way for All Intelligence," (September 19, 2024). Speech at Huawei Connect 2024, Shanghai, https://www.huawei.com/en/news/2024/9/hc-intelligent-era-xu.

NOTES

14. Nathan Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*, (2023). RAND Report, RRA853-1, Santa Monica, https://www.rand.org/pubs/research_reports/RRA853-1.html.
15. Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*, 2-3.
16. Miriam Matthews, Katya Migacheva, and Ryan Andrew Brown, *Superspreaders of Malign and Subversive Information on COVID-19: Russian and Chinese Efforts Targeting the United States*, (2021). RAND Report, Santa Monica, https://www.rand.org/pubs/research_reports/RRA112-11.html.
17. Mandiant, "M-Trends 2023," (February 14, 2024). Special Report, Reston, https://www.mandiant.com/m-trends; Microsoft Threat Intelligence, "Staying Ahead of Threat Actors in the Age of AI," *Microsoft Security Blog* (blog), https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai/.
18. Microsoft Threat Intelligence, "Staying Ahead of Threat Actors in the Age of AI."
19. Tim Niven, "The Evolution of China's Interference in Taiwan," (December 1, 2023). *The Diplomat*, https://thediplomat.com/2023/12/the-evolution-of-chinas-interference-in-taiwan/; Kimberly L. Wilson, "Strategic Responses to Chinese Election Interference in Taiwan's Presidential Elections," (Spring 2022). *Asian Perspective* 46, no. 2, https://doi.org/10.1353/apr.2022.0011, 255–77; Ella Apostoaie, "Bonnie Glaser and Ryan Hass on Getting Taiwan Policy Right," (September 24, 2023). *The Wire China*, https://www.thewirechina.com/2023/09/24/bonnie-glaser-and-ryan-hass-on-getting-taiwan-policy-right/.
20. *The Economist*, "China Is Flooding Taiwan with Disinformation," (September 26, 2023). Asia Section, https://www.economist.com/asia/2023/09/26/china-is-flooding-taiwan-with-disinformation.
21. Agust Börjesson and Yi-Chieh Chen, "The Political Split at the Heart of Taiwan's Struggle against Foreign Disinformation," (February 23, 2024). *Institute for Security & Development Policy*, https://isdp.eu/publication/the-political-split-at-the-heart-of-taiwans-struggle-against-foreign-disinformation/, 1.
22. Börjesson and Chen, "The Political Split at the Heart of Taiwan's Struggle against Foreign Disinformation, 1.
23. Börjesson and Chen, "The Political Split at the Heart of Taiwan's Struggle against Foreign Disinformation, 1.
24. Rishi Iyengar, "How China Exploited Taiwan's Election—and What It Could Do Next," (January 23, 2024). *Foreign Policy*, https://foreignpolicy.com/2024/01/23/taiwan-election-china-disinformation-influence-interference/.
25. *The Wall Street Journal*, "Taiwan Fights Onslaught of Chinese Disinformation Ahead of Key Election," (January 10, 2024). *Wall Street Journal Online*, video, 4:57, https://www.wsj.com/video/taiwan-fights-onslaught-of-chinese-disinformation-ahead-of-key-election/F6F0C406-164B-4572-86B0-F54736B2B163.
26. Seth G. Jones, *Russian Meddling in the United States: The Historical Context of the Mueller Report*, (2019). CSIS Brief, Washington, D.C.: Center for Strategic and International Studies, https://www.csis.org/analysis/russian-meddling-united-states-historical-context-mueller-report.
27. Adam B. Ellick, Adam Westbrook, and Jonah M. Kessel, "Meet the KGB Spies Who Invented Fake News," (November 12m 2018). *The New York Times*, video, 15:37, https://www.nytimes.com/video/opinion/100000006210828/russia-disinformation-fake-news.html.
28. Ellick, et al., "Meet the KGB Spies Who Invented Fake News."
29. Ellick, et, al., "Meet the KGB Spies Who Invented Fake News"; U.S. Department of State, *Pillars of Russia's Disinformation and Propaganda Ecosystem*, (August 2020). Washington, D.C.: Global Engagement Center, https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia's-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.
30. *The Wall Street Journal*, "Taiwan Fights Onslaught of Chinese Disinformation Ahead of Key Election."
31. AFP News, "Taiwan Voters Face Flood of Pro-China Disinformation," (January 10, 2024). *France 24*, https://www.france24.com/en/live-news/20240110-taiwan-voters-face-flood-of-pro-china-disinformation.
32. Clint Watts, "Same Targets, New Playbooks: East Asia Threat Actors Employ Unique Methods," *Microsoft Threat Analysis Center*, no. East Asia Report (April 4, 2024): 1–15, https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/.
33. Jennifer Creery, "Taiwan Builds Own AI Language Model to Counter China's Influence," (January 26, 2024). *The Japan Times*, Business Section, https://www.japantimes.co.jp/business/2024/01/26/tech/taiwan-ai-model-counter-china/.

NOTES

34. *AFP News*, "Taiwan Voters Face Flood of Pro-China Disinformation."
35. *AFP News*, "Taiwan Voters Face Flood of Pro-China Disinformation."
36. Douyin is a video sharing platform that is popular in China and is considered the mainland Chinese counterpart to TikTok. Both platforms are owned by the Chinese company ByteDance. Source: Claire Fu and Daisuke Wakabayashi, "There is No TikTok in China, but There Is Douyin. Here's What It Is," (April 25, 2024). *The New York Times Online*, Business Section, https://www.nytimes.com/2024/04/25/business/china-tiktok-douyin.html.
37. Fu and Wakabayashi, "There is No TikTok in China, but There Is Douyin. Here's What It Is."
38. *AFP News*, "Taiwan Voters Face Flood of Pro-China Disinformation."
39. Rishi Iyengar, "How China Exploited Taiwan's Election—and What It Could Do Next," (January 23, 2024). Foreign Policy, https://foreignpolicy.com/2024/01/23/taiwan-election-china-disinformation-influence-interference/.
40. Iyengar, "How China Exploited Taiwan's Election—and What It Could Do Next."
41. Dustin Volz, "China Is Targeting U.S. Voters and Taiwan With AI-Powered Disinformation," (April 5, 2024). *The Wall Street Journal*, Politics Section, https://www.wsj.com/politics/national-security/china-is-targeting-u-s-voters-and-taiwan-with-ai-powered-disinformation-34f59e21.
42. Iyengar, "How China Exploited Taiwan's Election—and What It Could Do Next."
43. Iyengar, "How China Exploited Taiwan's Election—and What It Could Do Next."
44. Patrick Tucker, "How China Could Use Generative AI to Manipulate the Globe on Taiwan," (September 10, 2023). *Defense One*, https://www.defenseone.com/technology/2023/09/how-china-could-use-generative-ai-manipulate-globe-taiwan/390147/.
45. Jennifer Creery, "Taiwan Builds Own AI Language Model to Counter China's Influence," (January 26, 2024). *The Japan Times*, Business Section, https://www.japantimes.co.jp/business/2024/01/26/tech/taiwan-ai-model-counter-china/.
46. Yixuan Lin, "Can Taiwan's First Mandarin LLM Prevent an Invasion of Chinese Mandarin AI?," (Janaury 31, 2024). *CommonWealth Magazine*, https://english.cw.com.tw/article/article.action?id=3614.
47. Lin, "Can Taiwan's First Mandarin LLM Prevent an Invasion of Chinese Mandarin AI?"
48. Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, "Chinese Disinformation Efforts on Social Media," (2021). RAND Research Report, Santa Monica, https://www.rand.org/pubs/research_reports/RR4373z3.html, l36; Iyengar, "How China Exploited Taiwan's Election—and What It Could Do Next."
49. Iyengar, "How China Exploited Taiwan's Election—and What It Could Do Next."
50. Iyengar, "How China Exploited Taiwan's Election—and What It Could Do Next."
51. An example of one team is the Disinformation Coordination Team who propose policy changes and balances upholding civil liberties with the nuances of the legal system, in regards to disinformation. Source: Kao Shih-Shiuan, "Taiwan's Response to Disinformation: A Model for Coordination to Counter a Complicated Threat," (September 16, 2021). T*he National Bureau of Asian Research (NBR)*, NBR Special Report, no. 93, 1–30, https://www.nbr.org/publication/taiwans-response-to-disinformation-a-model-for-coordination-to-counter-a-complicated-threat/.
52. Shih-Shiuan, "Taiwan's Response to Disinformation: A Model for Coordination to Counter a Complicated Threat."
53. Shih-Shiuan, "Taiwan's Response to Disinformation: A Model for Coordination to Counter a Complicated Threat."
54. Associated Press, "Taiwan Passes Law Targeting Chinese Political Interference," *AP News*, December 31, 2019, https://apnews.com/general-news-43e9cf4cd5190c6c296854f88cfbef78.
55. Associated Press, "Taiwan Passes Law Targeting Chinese Political Interference."
56. Shih-Shiuan, "Taiwan's Response to Disinformation."
57. Shih-Shiuan, "Taiwan's Response to Disinformation."
58. Shih-Shiuan, "Taiwan's Response to Disinformation."
59. Willian Hung, "Media Literacy Education: Taiwan's Key to Combating Disinformation," (March 6, 2024). *Global Taiwan Institute* 9, no. 5, https://globaltaiwan.org/2024/03/media-literacy-education-taiwans-key-to-combating-disinformation/.
60. Hung, "Media Literacy Education: Taiwan's Key to Combating Disinformation."
61. Hung, "Media Literacy Education: Taiwan's Key to Combating Disinformation."

NOTES

62. Hung, "Media Literacy Education: Taiwan's Key to Combating Disinformation."
63. Hung, "Media Literacy Education: Taiwan's Key to Combating Disinformation."
64. Patrick Tucker, "Taiwan Is Using Generative AI to Fight Chinese Disinfo," (September 22, 2023). *Defense One*, Science & Technology Section, https://www.defenseone.com/technology/2023/09/taiwan-using-generative-ai-fight-chinese-disinfo/390573/.
65. William Yang, "Q&A: Taiwan AI Labs Founder Warns of China's Generative AI Influencing Election," (January 5, 2024). Interview, *Voice of America*, https://www.voanews.com/a/q-a-taiwan-ai-labs-founder-warns-of-china-s-generative-ai-influencing-election-/7428717.html.
66. Yang, "Q&A: Taiwan AI Labs Founder Warns of China's Generative AI Influencing Election."
67. TAIDE is short for Taiwan's Trustworthy AI Dialogue Engine. Source: Lin, "Can Taiwan's First Mandarin LLM Prevent an Invasion of Chinese Mandarin AI?"
68. Yen-Ting Lin and Yun-Nung Chen, "Taiwan LLM: Bridging the Linguistic Divide with a Culturally Aligned Language Model," (November 20, 2023). Cornell University, arXiv, http://arxiv.org/abs/2311.17487.
69. Lin and Chen, "Taiwan LLM: Bridging the Linguistic Divide with a Culturally Aligned Language Model,
70. Lin, "Can Taiwan's First Mandarin LLM Prevent an Invasion of Chinese Mandarin AI?"; AIinAsia, "Taiwan's Quest for AI Autonomy: A Homegrown Language Model," (January 29, 2024). *AI in Asia* (blog), https://aiinasia.com/taiwan-builds-its-own-ai-language-model-to-fight-chinas-digital-influence-and-strengthen-taiwanese-identity/.
71. Lin and Chen, "Taiwan LLM;" AIinAsia, "Taiwan's Quest for AI Autonomy."
72. James Farrell, "Meta Shuts Down Thousands of Fake China-Based Facebook Accounts Aiming To Polarize U.S. Voters," (November 20, 2023). *Forbes*, https://www.forbes.com/sites/jamesfarrell/2023/11/30/meta-shuts-down-thousands-of-fake-china-based-facebook-accounts-aiming-to-polarize-us-voters/.
73. Vera Bergengruen, "Meta Takes Down 'Largest Ever' Chinese Influence Operation," (August 31, 2023). *TIME*, https://time.com/6310040/chinese-influence-operation-meta/.
74. Bergengruen, "Meta Takes Down 'Largest Ever' Chinese Influence Operations;" Farrell, "Meta Shuts Down Thousands Of Fake China-Based Facebook Accounts Aiming To Polarize U.S. Voters."
75. Microsoft Threat Intelligence, "Staying Ahead of Threat Actors in the Age of AI."
76. Microsoft Threat Intelligence, "Staying Ahead of Threat Actors in the Age of AI."
77. Microsoft Threat Intelligence, "Staying Ahead of Threat Actors in the Age of AI."
78. Microsoft Threat Intelligence, "Staying Ahead of Threat Actors in the Age of AI."
79. Kat Devlin and Christine Huang, *In Taiwan, Views of Mainland China Mostly Negative*, (May 12, 2020). Washington, D.C.: Pew Research Center, https://www.pewresearch.org/global/2020/05/12/in-taiwan-views-of-mainland-china-mostly-negative/; Christine Huang and Kelsey Jo Starr, "Most People in Taiwan See Themselves as Primarily Taiwanese; Few Say They're Primarily Chinese," (January 16, 2024). *Pew Research Center* (blog), https://www.pewresearch.org/short-reads/2024/01/16/most-people-in-taiwan-see-themselves-as-primarily-taiwanese-few-say-theyre-primarily-chinese/.
80. Alison Hsiao, "Taiwan-Developed Generative AI System Set to Benefit All Sectors - Focus Taiwan," (April 30, 2024). *Focus Taiwan - CNA English News*, https://focustaiwan.tw/sci-tech/202404300026.

Embracing Memory-Safe APIs for C2 Systems

Captain Brian Yarbrough, U.S. Air Force
Major Phelan Guan, U.S. Army

ABSTRACT

Information exchange between systems relies on secure implementation of Application Program Interfaces (APIs). This is especially true for modern Joint All-Domain Command and Control (JADC2) efforts. Unfortunately, many mission-critical systems implement APIs with programming languages that are not memory safe. We discuss how the use of these inherently insecure languages creates strategic and tactical risk for Department of Defense (DoD) command and control, artificial intelligence, and legacy systems. Furthermore, we present a set of recommendations for migrating to modern programming languages or mitigating risks from languages that lack memory safety.

INTRODUCTION

The National Defense Strategy directs the Joint Force to "gain and maintain information advantage, particularly in cyberspace, space, and the electromagnetic spectrum."[1] Realizing and implementing Joint All Domain Command and Control (JADC2) is the Joint Force plan to do this by guiding commanders to "sense, make sense, and act" in the operational environment.[2] Four of the five JADC2 lines of effort – establish the data enterprise, establish the technical enterprise, integrate with nuclear C2, and modernize mission partner information sharing – hinge on the ability to share information between systems securely, quickly, and robustly.

Captain Brian Yarbrough is a U.S. Air Force Cyber Warfare Operations Officer. He graduated from the U.S. Air Force Academy in 2016 and has a Master of Computer Engineering from Northeastern University. While an MIT Lincoln Laboratory Fellow he conducted research on agent-based decision support for resilient cyber-physical systems. He has also been assigned to The Defense Digital Service and Special Operations Command. He currently instructs Electrical and Computer Engineering at the U.S. Air Force Academy. His primary research interests include embedded systems, artificial intelligence, and multiagent systems.

Effective data sharing among information systems occurs through Application Programming Interfaces (APIs) that standardize inputs and outputs of a system given certain mission or business parameters. APIs must provide confidentiality, integrity, and availability to the warfighter. Just as a house must sit upon a solid foundation, programming these APIs must rest upon a programming language that doesn't take unnecessary risks when it comes to memory and type safety, lest it fall victim to a raft of vulnerabilities that plague even the top Silicon Valley tech companies.

We present the recommendations of this paper as part of a larger holistic strategy for defending DoD information systems; it is not a silver bullet against all cyber-attacks, but rather is narrowly focused to disrupt specific links in an adversary's attack chain. These recommendations would enable DoD to raise the cost of a successful cyber-attack, to the point where it may frustrate would-be attackers, or draw resources away from attacks against other potential U.S. Government (USG) targets. Not modernizing DoD language standards carries an equally impactful cost: the loss of speed, time, and trust in our warfighting decision systems.

STRATEGIC THREAT ASSESSMENT AGAINST DOD WARFIGHTING SYSTEMS

There are three major categories of DoD warfighting systems that we view as significantly vulnerable to threats: Command and Control (C2), Artificial Intelligence (AI), and legacy information systems. We couch threats to each category of systems in terms of Confidentiality, Integrity, and Availability – often referred to by cybersecurity professionals as the "CIA Triad."

Depending on the application, one leg of the CIA triad may outweigh the others; for example, a weather website likely cares more about availability than confidentiality. However, for C2 systems, an adversary may drastically impede military operations by impacting

Major Phelan Guan is a U.S. Army Cyber Warfare Operations Officer who served in various capacities throughout the U.S. Cyber Mission Force and Special Operations Command, including a joint force headquarters, deployed joint task force, and a cyber protection team, with operational and combat deployments to Senegal and Afghanistan. He graduated from the United States Military Academy in 2013 with a B.S. in Information Technology and earned an M.S. in Analytics from Georgia Institute of Technology in 2022.

any single leg of the triad. Examples of this include:

- **Confidentiality:** an adversary can know sensitive plans or details of military forces or operations.
- **Integrity:** an adversary can manipulate a com mander's orders, causing confusion or unintend ed actions.
- **Availability:** an adversary can deny or disrupt a commander's ability to communicate with forces.

Command and Control

> In the current global security environment, the United States military faces agile adversaries who increasingly seek to undermine our strategic and operational strengths by impeding, and, where possible, denying our command and control (C2) capabilities. The ability of the U.S. military to regain and maintain information and decision advantage is one of the Department's top priorities.[3]
>
> – Joint All-Domain Command & Control (JADC2) Strategy

JADC2 was designed to connect sensors from all military services into a single network. The ride-sharing service Uber offers an analogy: Uber combines two different apps (one for drivers, and the other for riders) to provide a service (ride sharing).[4] The Air Force is developing the Advanced Battle Management System (ABMS), while the Army and Navy are developing Project Convergence and Project Overmatch, respectively. All these systems aim to combine multiple applications to provide warfighting capability, forming the C2 backbone of the future. However, how would data from an Army sensor make its way to an Air Force planning tool within JADC2?

The standard way for information systems to exchange information is via an API. Any C2 platform must reliably transfer and share data using APIs. In

order for a component commander to have reliable, trustworthy awareness of a battlespace, the data must be available and confidential and their contents cannot have not been altered.

The danger of any breach of C2 systems is so obvious it almost does not bear comment. Simply put, a cyber-attack on our C2 enables an adversary to follow Sun Tsu's advice: "Success in warfare is gained by carefully accommodating ourselves to the enemy's purpose."[5] Therefore, since APIs are the main "avenues of approach" into an information system, the utmost care should be put into their design and execution.

Artificial Intelligence

As discussed by the authors of the best-selling book *Prediction Machines*, Artificial Intelligence (AI) is at its core a revolution in cheap prediction, which "takes information you have, often called 'data,' and uses it to generate information you don't have."[6] Commanders and other decision makers can use AI predictions to reduce uncertainty and thereby mitigate risk.

If a commander is going to rely on AI to assist in decision making, both the commander and the AI must have the right data available for consumption. That means granting AI access to C2 systems, weather and map data, radio transmissions — anything a commander and staff would have access to. Again, we see the primary way for digital information systems to reliably exchange data is through APIs, and analog data sources may soon have a corresponding digital "translator" that will also send its data digitally via APIs.

Furthermore, the AI generated predictions must be trustworthy: they must be appropriately confidential and maintain their integrity so the commander can be sure the adversary isn't privy to the AI's assistance, and that it has not been modified or tampered with. According to MITRE, if an adversary can exploit or poison any component of the AI pipeline, particularly the interfaces exchanging data, they can manipulate the behavior of a system to serve a malicious goal.[7]

Legacy Systems

An analysis of memory bugs in the Android operating system found that critical vulnerabilities are identified in newer code more frequently than in older code, presumably because older code has had more time to have bugs caught and repaired.[8] Unfortunately, this is not the case for many DoD systems.

For government systems, code updates are seldom made after completion of the initial contract because updates require a new contract. While program such as Hack the Pentagon[9] have opened the door for security researchers to responsibly disclose bugs on some unclassified systems, classified systems are (understandably) not part of any public vulnerability disclosure and tracking process. As a result, it is unlikely that older bugs are ever identified or fixed even if they are identified.

Legacy systems present a particularly unique challenge to the DoD because it is difficult to tell how they are intertwined with other systems. A simple security update may cause unexpected

and difficult-to-diagnose errors. However, it is exactly this interconnectedness that pairs with their inherent vulnerabilities that makes legacy systems a particularly lucrative target for attackers. This is true even for legacy systems that are not deemed mission-critical because an adversary may be able to use the system as a beachhead and then move laterally to more critical systems. Our most vulnerable systems are oftentimes the ones by which an adversary can do the most harm.

TACTICAL RISK ASSESSMENT

Having discussed why C2, AI, and legacy systems present the greatest vulnerabilities to strategic cyber threats, we will now discuss a tactical avenue into accessing these systems: APIs. in particular, how APIs implemented using non-memory-safe programming languages present high risk targets. We borrow this risk assessment method from NIST SP 800-30 — the USG's official guidance for conducting risk assessments of federal information systems — which expresses risk as a matrix combining the likelihood of the threat with the level of impact.[10] In order to quantify likelihood and impact, we first present background on modern server communication, what makes APIs a likely attack surface, and the impact of adversary remote code execution (RCE).

Servers and APIs

Well-designed information systems are frequently built from modular subsystems. The popular three-tier paradigm includes a user interface (presentation layer), logic (application and business layer), and data access (database layer).[11] Each subsystem must transfer data between the other subsystems, without working knowledge of how another subsystem operates. This transfer is accomplished via an application program interface (API). In this way, a subsystem can treat anything behind an API as a 'black box.' All any subsystem needs to know about another is the correct inputs and what to expect as the output. As a result of this modularity, the actions from a user clicking through a website can be replicated or manipulated programmatically by directly interacting with the logic layer.

APIs are also frequently used for two independent systems to communicate with each other. For example, the company Stripe provides an API so that you can purchase a product from a website without that website actually seeing your credit card information.[12] Of course, this API must be written in a programming language and must then run on a server. The implementation of an API and the server on which it runs are the primary attack surfaces that we are concerned with in this paper.

APIs as an Attack Surface

Since APIs are the public face of an information system, they can never be fully closed off from an adversary or the system would be useless. As such, it stands to reason that an adversary will frequently target this attack surface. As we previously stated, API's are

regarded as black boxes that correctly process data given specified inputs. API security is a large topic and should be considered a component towards achieving a zero-trust architecture to increase resiliency and readiness to counter cyber threat actors.[13] For example, API best practices include using Transport Layer Security (TLS) encryption, sound authentication and authorization, avoiding sensitive information in URLs, narrow definition of requests and responses, and continuous monitoring.[14] Within the NIST 800-30 framework, we estimate that 81% of likely cyber attacks are APIs of web applications,[15] giving us a high likelihood of threat event initiation. Combined with a high likelihood that an exploited vulnerability would result in adverse impacts, we find the overall NIST 800-30 likelihood score to be "high."

However, there is less literature concerning the specific programming language with which an API is implemented. We argue that writing APIs in a language that implements certain safeguards, particularly memory safety, results in a significantly more secure API.

Dangers of RCE

"Hacking" an API involves providing unexpected inputs in such a manner that the API exposes confidential data or executes unauthorized snippets of code. It is these unauthorized snippets of code (also known as Remote Code Execution, or RCE in cybersecurity parlance) that pose the greatest risk to the information system, the decision maker, and by extension, the warfighter. The primary way RCE is achieved on APIs is through unsanitized inputs – we can see that in CISA's twelve most routinely exploited vulnerabilities, four of them are from unsanitized inputs, all resulting in RCE.[16] Exposed data may impact the 'confidentiality' leg of the CIA triad, but RCEs threaten all three legs of the triad since an adversary can cause the server to perform actions the server would otherwise not. Drawing back on the NIST 800-30 impact framework, we can expect a threat event to DoD systems to have serious to catastrophic adverse effects to operations, service members, and the Nation. As such, depending on the individual system, RCEs could have a 'moderate' to 'very high' NIST impact score.

Memory Unsafe Code is an Unnecessary Risk

Microsoft, Google, and numerous other big-tech companies have openly stated that memory errors contribute to approximately seventy percent of software vulnerabilities.[17,18] Here is a small sample of software vulnerabilities from the last three years that could have been mitigated by the usage of a memory safe language.

- Two different heap overflows in Chromium impacted Chrome and Edge browsers as well as iOS and were exploited in the wild.[19,20]
- A buffer overrun in X.509 certificate verification – the certificates that provide the encryption for an HTTPS website, among other things – allowed for potential remote code execution; however, in this specific case many platforms already implemented stack overflow protection, which mitigated the issue.[21] This type of protection is included in the Recommendations section below.[22]

- Google's Project Zero identified a buffer overflow in Libgcrypt, a critical component of encryption for Linux systems, that allowed an attacker to crash a system.
- Apple has struggled with an actively exploited buffer overflow in its kernel[23] that has been patched and repatched in multiple releases of iOS.[24]

Attacks that function by exploiting a lack of type-safety are also prevalent.

- A 2023 type confusion bug in Google Chrome allowed remote exploitation.[25]
- A 2023 type confusion bug in OpenSSL, one of the most popular encryption libraries in the world, allowed an attacker to read sensitive memory contents.[26]
- An advanced persistent threat (APT) dubbed "Sidewinder" and assessed to be an Indian threat actor group[27] frequently uses a technique called polymorphism to take advantage of type manipulations and evade antivirus software.[28]

These examples demonstrate that even the best technology organizations in the world — commercial and open source — struggle to implement memory and type controls properly when using an inherently unsafe language. It is incomprehensible that software built for the DoD using these same unsafe languages such as C or C++ could be much better, especially considering the singular focus and resources commercial technology companies command. To apply the NIST 800-30 risk matrix: when we take the 'high' likelihood a cyber adversary interacting with an API, and that API is written in a memory and type unsafe language that leads to a 'moderate' to 'very high' impact RCE, we can see the total risk to a system is 'very high.' Given that there are memory and type safe languages that by design prevent these vulnerabilities from existing in the first place, allowing DoD information systems to be written in memory and type unsafe languages is an unnecessarily high risk.

RECOMMENDATIONS

Considering the above threat assessment, NSA and NIST recommendations, and industry trends, the DoD should ensure that its APIs are newly implemented or rewritten in an appropriate programming language. If rewriting an API is infeasible, the system should implement alternative mitigations. Furthermore, most new DoD projects should not be written in C/C++.

> NSA advises organizations to consider making a strategic shift from programming languages that provide little or no inherent memory protection, such as C/C++ and assembly, to a memory safe language when possible.[29]

Below, we provide additional detail on this recommendation and how it may be implemented.

Select an Appropriate Programming Language

Whether beginning a new project or selecting a language to rewrite a piece of an existing project, it is critical to select an appropriate programming language. Memory safety is the

most important trait, but we also provide general characteristics that make a programming language a more compelling choice than others. Desirable traits beyond memory safety include type safety, compilation, maintainability, and the support of an active community. Examples of languages that meet all our recommended criteria include Go, Rust, and Kotlin.

Memory Safety

According to NSA, "Memory safety is a broad category of issues related to how a program manages memory. One common issue is called a "buffer overflow," where data are accessed outside the bounds of an array. Other common issues relate to "memory allocation."[30] A simple example of a buffer overflow is if a programmer asks a user to enter their first name and they expect, at most, fifteen characters but an attacker can insert an arbitrary number of characters followed by malicious code.

Memory safe programming languages can help prevent programmers from introducing certain memory bugs because they automatically manage memory and implement guardrails that mitigate common vulnerabilities.

Using memory safe language provides such a security advantage that in response to Executive Order 4028, NIST published NISTIR 8397, which included the recommendation: "Where practical, use memory-safe languages and limit disabling memory safety mechanisms."[31]

Type Safety

Type-safe languages prevent operations on values that are not of the appropriate data type. This means that a programmer cannot do a nonsensical operation such as *x* = "*apple*"-3.

Type checks prevent logical programming bugs and can also provide security value.[32] Microsoft lists "type confusion" as the third leading cause for software vulnerabilities because specific data types are allocated a specific amount of memory and incorrect pointers to or operations on this memory can lead to code execution.[33]

Recent examples of type-safety exploits include:

- A 2023 type confusion bug in Google Chrome allowed remote exploitation.[34]
- A 2023 type confusion bug in OpenSSL, one of the most popular encryption libraries in the world, allowed an attacker to read sensitive memory contents.[35]
- An advanced persistent threat (APT) dubbed "Sidewinder" and assessed to be an Indian threat actor group[36] frequently uses a technique called polymorphism to take advantage of type manipulations and evade antivirus software.[37]

In addition to improving security, type-safe languages result in more reliable and resilient software because more errors are caught in development instead of in production. Type safety also aids maintainability by helping developers understand what is happening in the software. This is particularly the case with statically typed languages, meaning that a

variable's type is determined when the code is built, rather than when it is run. Again Go, Rust, and Kotlin are languages that meet this criterion.

It should be noted that some developers feel writing type-safe code can be slower. The flexibility of Python's dynamic type system is part of the reason it is hugely popular for prototyping. Yet even the most zealous Python advocates acknowledge that static typing can make programs easier to understand, detect bugs earlier, and improve productivity.[38]

Compilation

Compilation is the process of converting a high-level code into machine code that can be directly executed. Modern compilers make guarantees about a program before it can be built. This means that many errors are caught in development rather than causing bugs in production. Additionally, interpreted languages convert human-written programs into machine code dynamically, requiring memory to be both executable and writable at runtime, which allows for many forms of code injection to RCE.[39] These sorts of protections are available and enforced in modern compilers.

Designed for Maintainability

It is well known that most of the cost (about 70%) associated with a software program will go towards its maintenance.[40] There is no single accepted definition for code quality; nonetheless, there are various efforts to quantize code quality with the hopes that higher-quality code can be maintained with less investment. Some of these metrics include defects, testing coverage, cyclomatic complexity, and understandability.[41] Here we pay special attention to understandability as it contributes to maintainability.

As the adage goes: code is read many more times than it is written. The readability of code is an important factor in maintainability.[42] In the same way that someone can quickly scan a newspaper because the paper tends to adhere to a common format, adherence to language standards aids in the production of high-quality code with minimum ambiguity and misunderstanding.[43] While older programming languages do not enforce a standard format, both Go and Rust offer officially supported format tools that standardize indentation, alignment, and style.[44,45] Beyond formatting, we again see benefits of aforementioned static type systems: type annotations aid a developer in understanding a program's functions.[46]

Supported by an Active Community

A large community behind a programming language results in a healthier ecosystem. Actively supported languages will have more libraries available; the chances of bugs being detected and remediated is greater; hiring experienced developers will be easier; there will be more resources such as tutorials, podcasts, or conferences about the language. To leverage these benefits, manage costs, and avoid vendor lock-in, the public sector should almost never develop its own programming languages.

One of the most well-regarded surveys in the field, Stack Overflow's *Developer Survey*, lists languages in terms of popularity. Of the memory-safe languages reported in 2023,[47] the most popular languages for developing user-facing websites remain JavaScript, HTML/CSS, and TypeScript. For server development, Go, Rust, and Kotlin are the most popular of the comparable languages.[48] The source code for each of these languages is publicly available on GitHub, allowing for community input and concurrence for the language's continued growth, expansion of capabilities, and security corrections.

Rewrite code

Where feasible, rewriting C and C++ code is the preferred solution because this will result in more secure, stable, and correct applications. However, rewriting an entire application is often infeasible. In this case, triage the components of an application and prioritize rewriting the functions that process incoming data from an API. Once deserialized and sanitized by a memory-safe program, the result can be handed to the rest of the C/C++ application with greater confidence.

Microsoft took this approach in a Rust rewrite of the Windows DirectWrite package, which renders fonts. DirectWrite was "notorious for security issues" precisely because its primary job was to process arbitrary incoming data. After the rewrite, which took two developers six months and involved 152-thousand lines of Rust and 96-thousand lines of C++, developers saw no regressions on logic errors and a modest performance boost.[49]

ALTERNATIVE MITIGATIONS

Adding a second language to any project does increase complexity. The requirements to build the application increase. Testing must be redone. So, although a robust solution, there will be instances where it is not appropriate to rewrite part of an application. In this case employ other mitigation strategies.

Sandbox Code

If code is written in C/C++ and parses untrustworthy input, it should be contained within a tightly constrained and unprivileged sandbox.[50] The Android platform has taken this approach, and while it has not reduced the number of vulnerabilities, it has reduced their severity.[51] A properly implemented sandbox means that if an attacker exploits a memory bug (or another bug) then she will be unable to impact the larger application without chaining exploits together. This increases the difficulty of exploitation, but chaining exploits is well within the realm of possibility for sophisticated adversaries. Unfortunately, sandboxing also consumes additional overhead and introduces latency.

A sandboxed piece of an application must be able to operate as a service, independently from the rest of the system. Service-oriented architecture provides the benefits of encapsulation, scalability, and ease of change.[52] As discussed by 18F, the digital expert team within the

General Services Administration (GSA), many government systems are originally designed as a monolithic architecture.[53] Thus, some applications may require significant code rewrites just to get them to a place where sandboxing as a service is even achievable.

Recompile Code

In situations where rewriting or sandboxing code is not viable, some risk mitigation can still be reaped by recompiling existing C/C++ code with tools like AddressSanitizer. Google developed AddressSanitizer to be a fast memory-error detector.[54] It works by recompiling C/C++ code and then mapping and monitoring memory. This does introduce runtime overhead — meaning programs typically execute about half as fast — but there are no false positives. Google has extensively used AddressSanitizer to find and fix bugs in Chromium, significantly enhancing the browser's security and stability.

AddressSanitizer is supported by GCC and CLANG, two ultra-popular compilers, and is readily integrated with existing workflows.[55,56] However, it's crucial to note that AddressSanitizer is not a silver bullet. It cannot detect all types of memory errors and does not eliminate the need for other security measures like code reviews and comprehensive testing. Still, as a part of a multi-layered security strategy, it provides a valuable layer of defense against memory safety vulnerabilities.

Decommission Legacy Systems

One of the DoD's greatest options for decreasing risk from memory bugs is eliminating problematic legacy systems. In the face of a constricting budget there can be resistance to eliminating systems that seem to function. But there is a hidden cost to keeping legacy systems around. For instance, the DoD pays Microsoft millions of dollars to continue some basic support for Windows XP, which reached official end-of-life in 2014.[57] Interoperability becomes an ever-larger burden, and making even a small change or upgrade can be an insurmountable task.

DoD should scour its systems for components that are used by a few straggling systems and force the final migration of those systems. The military spends millions of dollars on IT modernization, but often fails to migrate legacy systems fully to the new stack. As a result, the department is burdened with operating and maintaining a continually increasing number of systems to do the same task.

> When we speak of "legacy systems" in government, it does not mean simply that they are old. It means that we are grappling with the legacy of decades of competing interests, power struggles, creative work-arounds, and make-dos that are opportune at the time but unmanageable in the long run.
>
> — Recoding America[58]

We acknowledge that decommissioning legacy systems is not a simple task. Some senior leaders feel that the risks in changing a mission-critical legacy system are too great.[59] But this thinking is flawed. Instead, mission-critical systems must be updated precisely because their failure is unacceptable and our adversaries are actively seeking to induce such a failure.

Legacy systems should be replaced, and fully — but also gradually and with care. In the analysis "Starting Simple with JADC2," MITRE recommends that "a successfully engineered complex system should start with a simple working system, and then grow in complexity."[60] JADC2 cannot be built by bidding out full-scale replacements or development of complex systems. Rather, DoD should roadmap core services that should be decommissioned, review and update the policy that dictates their operation, and then allow for their agile completion in a federated manner.

REFUTATION

Even in a world where migration to memory-safe programming languages goes smoothly, there is no panacea for cybersecurity. Security vulnerabilities will still exist, whether they be caused by issues in logic, permissions, or architecture.

For example, Ethereum — which is the second most popular cryptocurrency behind Bitcoin — suffered a hack of its Decentralized Autonomous Organization (DAO) that resulted in the loss of $50-million.[61] This vulnerability arose from a recursive call bug[62] in a single line of code within an API call.[63] The Ethereum DAO is written in Solidity, which is a memory-safe and type-safe programming language.[64]

The loss of tens-of-millions of dollars was caused by programmer logic error and would not have been prevented by simply using a safer programming language. Rather, this emphasizes the importance of peer-review and frequent security testing of software; again, as part of a holistic strategy.

Comparison to the Failed Ada Mandate

The DoD has previously mandated language usage. The 1991 Department of Defense Appropriations Act stipulated that "where cost effective, all Department of Defense software shall be written in the programming language Ada, in the absence of special exemption by an official designated by the Secretary of Defense."[65] The Ada programming language implements memory and type safety as well as other compile-time checks. These and other features of the Ada language collectively make Ada a top pick for safety-critical and high integrity systems even today. However, the Ada Mandate faced massive pushback, included numerous exemptions, and was ultimately rescinded less than a decade after it took effect.[66]

Considering this, one might ask why our recommendation of mandating the use of memory-safe programming languages is any different. The downfall of the Ada Mandate was that it prescribed a single language for all applications. Furthermore, that language did not have

a developed toolchain or large community. As such, Ada was frustrating to work with and was a poor fit for some applications. Our recommendations for language selection identify characteristics which the language should have, but do not specify the language itself. This will provide greater flexibility and success than the Ada Mandate did, while still providing gains in security and maintainability.

CONCLUSION

The comprehensive analysis presented in this article underscores the crucial need for DoD to modernize its approach to software development, particularly in the realm of cybersecurity. The strategic vulnerabilities identified in Command and Control (C2) systems, Artificial Intelligence (AI) applications, and legacy information systems are vulnerabilities that can be exploited by adversaries, undermining the integrity, confidentiality, and availability of critical military operations. The critical role of APIs in these systems for interoperability makes them a focal point for both threats and mitigation efforts. As officially recommended by the U.S. White House, "in most cases, using memory safe programming languages is the most efficient way to substantially improve software security.[67]

Furthermore, the discussions of memory- and type-safety vulnerabilities are not constrained to the DoD. Both the public and private sectors rely extensively on APIs to communicate between systems and conduct business logic. The specificity of our analysis concentrated on DoD applications more richly develops our recommendations which are broadly applicable to reducing the cyber attack surface of information systems and should be widely adopted.

Our recommendation for the DoD to transition towards memory-safe and type-safe programming languages for new projects and, where feasible, rewrite existing code. It is not just a strategic necessity but a proactive step towards bolstering and assuring our national defense capabilities. Employing appropriate, modern, safe languages for developing the most critical components of DoD information systems will be critical to the successful achievement of JADC2 and fulfillment of the DoD Cyber Strategy.

ACKNOWLEDGMENTS

This work began as part of Air University Advanced Research at Squadron Officer School. Thank you to the staff for feedback on initial outlines.

DISCLAIMER

The views expressed in this article are those of the authors and do not necessarily reflect the official policy or position of the United States Air Force Academy, the United States Military Academy, the Department of Air Force, the Department of the Army, the Department of Defense, or the U.S. Government.

NOTES

1. U.S. Department of Defense (DoD), *Summary of the Joint All-Domain Command & Control (JADC2) Strategy,* (March 17, 2022). https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF, 3.
2. DoD, *JADC2 Strategy*, 4.
3. DoD, *JADC2 Strategy*, 1.
4. Congressional Research Service. "Joint All-Domain Command and Control (JADC2)," (January 21, 2022). https://sgp.fas.org/crs/natsec/IF11493.pdf, 1.
5. Sun Tzu, *The Art of War,* (2011). New York: Fall River Press. Translated by Lionel Giles, 224.
6. Ajay Agrawal, Joshua Gans, and Avi Goldfarb. *Prediction Machines: The Simple Economics of Artificial Intelligence*, (April 17, 2018). Boston, Massachusetts: Harvard Business Review Press, 24.
7. Mitre Atlas, "Adversarial Machine Learning 101." (March 2024), Mitre Atlas Website v4, 1.0. https://atlas.mitre.org/resources/adversarial-ml-101/.
8. Jeff Vander and Stephen Hines, "Rust in the Android Platform." (April 6, 2021), *Google Online Security Blog.* https://security.googleblog.com/2021/04/rust-in-android-platform.html.
9. U.S. Defense Digital Service and Chief Digital and Artificial Intelligence Office (CDAO), "Hack the Pentagon." https://www.hackthepentagon.mil/.
10. National Institute of Standards and Technology (NIST), S*pecial Publication (SP) 800-30 Revision 1, Guide for Conducting Risk Assessments*, (September 2012). https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf, I-1.
11. Eckerson, Wayne W. "Three Tier Client/Server Architecture: Achieving Scalability, Performance, and Efficiency in Client Server Applications," (January 1995). *Open Information Systems* 10, 1: 3(20).
12. Stripe, "Stripe API Reference," (accessed July 31, 2024). https://stripe.com/docs/api.
13. NIST, SP 800-30 R1, B-4. Defense Information Systems Agency (DISA), *DISA Next Strategy: Fiscal Year 2025 - 2029*, (May 1, 2024). DISA, https://www.disa.mil/-/media/Files/DISA/About/DISA-Next-Strategy-2025-2029.ashx, 27.
14. Abigail Ojeda, 2023. "REST API Security Best Practices," (November 15, 2023). *Akamai*, https://www.akamai.com/blog/security/rest-api-security-best-practices.
15. VaaData, "How to Strengthen the Security of Your APIs to Counter the Most Common Attacks?" (April 20, 2022). https://www.vaadata.com/blog/how-to-strengthen-the-security-of-your-apis-to-counter-the-most-common-attacks/
16. Cybersecurity Infrastructure Security Agency (CISA), "2022 Top Routinely Exploited Vulnerabilities." (August 3, 2023). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-215a.
17. Cybersecurity Infrastructure Security Agency (CISA), "The Urgent Need for Memory Safety in Software Products," (September 20, 2023). https://www.cisa.gov/news-events/news/urgent-need-memory-safety-software-products.
18. The Chromium Project, "Memory Safety, (accessed September 5, 2024).https://www.chromium.org/ Home/chromium-security/memory-safety/.
19. Microsoft Security Response Center (MSRC), "Chromium: CVE-2023-5217 Heap Buffer Overflow in Vp8 Encoding in Libvpx," (last updated October 20, 2023). https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-5217.
20. NIST, "CVE-2023-4863 Detail, Heap Buffer Overflow in libwebp in Google Chrome," (last modified July 31, 2024). National Vulnerability Database, https://nvd.nist.gov/vuln/detail/CVE-2023-4863.
21. NIST, "CVE-2022-36902 Detail, Jenkins Dynamic Extended Choice Parameter Plugin 1.0.1 and Earlier," (last modified November 2, 2023), https://nvd.nist.gov/vuln/detail/CVE-2022-36902.
22. Project Zero, "GPG Heap Buffer Overflow in Libgcrypt." (last updated February 11, 2021). Chromium Creative Commons, Google Developer Program. https://project-zero.issues.chromium.org/issues/42451258.
23. Apple, "CVE-2021-1816," (September 8, 2021). https://www.cve.org/CVERecord?id=CVE-2021-1816.
24. Apple Support, "About the Security Content of IOS 14.7 and IPadOS 14.7," (November 6, 2023). https://support.apple.com/en-us/103139.
25. NIST, "CVE-2023-3079, Type Confusion in V8 in Google Chrome," (last modified June 28, 2024). https://nvd.nist.gov/vuln/detail/CVE-2023-3079.
26. NIST, "CVE-2023-0286, Type Confusion Vulnerability, X.400 Address Processing Inside an X.509 GeneralName," (last modified February 4, 2024). https://nvd.nist.gov/vuln/detail/CVE-2023-0286.

NOTES

27. MITRE,"Sidewinder, T-APT-04, Rattlesnake, Group G0121," (last modified April 11, 2024). https://attack.mitre.org/groups/G0121/.
28. BlackBerry Threat Research and Intelligence Team, "SideWinder Uses Server-Side Polymorphism to Attack Pakistan Government," (May 8, 2023). https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan.
29. National Security Agency (NSA), "Software Memory Safety," (April 27, 2023). https://media.defense.gov/2023/Apr/27/2003210083/-1/1/0/CSI_SOFTWARE_MEMORY_SAFETY_ V1.1.PDF, 5-6.
30. NSA, "Software Memory Safety," 2.
31. Paul Black, Barbara Guttman, and Vadim Okun, "Guidelines on Minimum Standards for Developer Verification of Software," (October 2021). https://doi.org/10.6028/nist.ir.8397, 10.
32. Michal Aiban, ed., "Type Safety in Programming Languages," (last updated March 18, 2024). Baeldung Company Website, https://www.baeldung.com/cs/type-safety-programming.
33. Jeong Wook Oh, "Understanding Type Confusion Vulnerabilities: CVE-2015-0336," (June 18, 2015). Microsoft Security Website, https://www.microsoft.com/en-us/security/blog/2015/06/17/understanding-type-confusion-vulnerabilities-cve-2015-0336/.
34. NIST, CVE-2023-3079.
35. NIST, CVE-2023-0286.
36. MITRE, "Sidewinder, T-APT-04, Rattlesnake, Group G0121."
37. BlackBerry Threat Research and Intelligence Team, "SideWinder Uses Server-Side Polymorphism to Attack Pakistan Government."
38. MyPy, "Frequently Asked Questions." (accessed December 18, 2023). https://mypy.readthedocs.io/en/latest/faq.html.
39. Eric Jaeger and Olivier Levillain, "Mind Your Language(s): A Discussion about Languages and Security," *IEEE Security and Privacy Workshops,* (May 17, 2014). https://www.ieee-security.org/TC/SPW2014/papers/5103a140.PDF, 146.
40. Dennis D. Smith, *Designing Maintainable Software,* (May 28, 1999). New York: Springer, 3.
41. Herb Krasner, "The Cost of Poor Quality Software in the US: A 2018 Report," (September 26, 2018). *Consortium for IT Software Quality (CISQ)*, Carnegie Mellon University, https://www.it-cisq.org/wp-content/uploads/sites/6/2023/09/The-Cost-of-Poor-Quality-Software-in-the-US-2018-Report.pdf. 29.
42. K.K. Aggarwal, Yogesh Singh, and Jitender K. Chhabra, "An Integrated Measure of Software Maintainability," (2002). *Annual Reliability and Maintainability Symposium*, Proceedings (Cat. No.02CH37318). https://doi.org/10.1109/rams.2002.981648, 1.
43. Mohammad Abdallah and Mustafa Alrifaee, "A Heuristic Tool for Measuring Software Quality Using Program Language Standards," (May 3, 2022). *The International Arab Journal of Information Technology Vol. 19. No. 3*, pp. 314-322, https://doi.org/10.34028/iajit/19/3/4, 314.
44. The Go Project, "Gofmt Command," Pkg.go.dev. (Accessed December 5, 2023). Google Open-Source Project, Distributed under BSD-Style License, https://pkg.go.dev/cmd/gofmt.
45. GitHib, Rust Language Site, "Rustfmt," (Accessed December 18, 2023). https://github.com/rust-lang/rustfmt.
46. Stefan Hanenberg, Sebastian Kleinschmager, Romain Robbes, Éric Tanter, and Andreas Stefik, "An Empirical Study on the Impact of Static Typing on Software Maintainability," (December 11, 2013). *Empirical Software Engineering, Volume 19*, 1335–82. https://doi.org/10.1007/s10664-013-9289-1, 5.
47. Stack Overflow Company Site, "Stack Overflow Developer Survey 2023," (May 2023). https://survey.stackoverflow.co/2023/#section-most-popular-technologies-programming-scripting-and-markup-languages.
48. The survey shows Java as more popular than Kotlin; this is partly due to the age of Java. Kotlin addresses several persistent issues in Java such as null references and shortcomings of the type system. https://kotlinlang.org/docs/comparison-to-java.html#what-kotlin-has-that-java-does-not.
49. David Weston, "BlueHat IL 2023 – David Weston – Default Security," Microsoft, (April 19, 2023). https://youtu.be/8T6ClX-y2AE?si=mWGnF5Y6HY8UUnDm.
50. Jeff Vander Stoep and Stephen Hines, "Rust in the Android Platform," (April 6, 2021). Google Security Blog, https://security.googleblog.com/2021/04/rust-in-android-platform.html.

NOTES

51. Jeff Vander Stoep and Chong Zhang. "Queue the Hardening Enhancements," (May 9. 2019). Android Developers Blog, https://android-developers.googleblog.com/2019/05/queue-hardening-enhancements.html.
52. Martin Kleppmann, *Designing Data-Intensive Applications: The big ideas behind reliable, scalable, and Maintainable Systems*, (May 2, 2017). Sebastopol, California: O'Reilly Media, 132.
53. Kane Baccigalupi, "The Best Way to Build Big Is to Start Small," (January 11, 2017). *18F – Digital Service Delivery, General Services Administration*, https://18f.gsa.gov/2017/01/11/the-best-way-to-build-big-is-to-start-small/.
54. Konstantin Serebryany, Derek Bruening, Alexander Potapenko, and Dmitry Vyukov, "AddressSanitizer: A Fast Address Sanity Checker," (June 13, 2012). USENIX Annual Technical Conference 2012, https://www.usenix.org/system/files/conference/atc12/atc12-final39.pdf.
55. The GNU Compiler Collection (GCC), "Instrumentation Options (Using the GNU Compiler Collection)," (accessed September 5, 2024). https://gcc.gnu.org/onlinedocs/gcc/Instrumentation-Options.html.
56. CLANG, "AddressSanitizer – Clang 12 Documentation," LLVM, (accessed September 5, 2024) https://clang.llvm.org/docs/AddressSanitizer.html.
57. Jeremy Hsu, "Why the Military Can't Quit Windows XP," (June 4, 2018). *Slate Magazine*. https://slate.com/technology/2018/06/why-the-military-cant-quit-windows-xp.html.
58. Jennifer Pahlka, Recoding America: *Why Government is Failing in the Digital Age and How We Can Do Better*, (June 13, 2023). New York: Metropolitan Books, Kindle, loc 524.
59. Jane Edwards, "Thomas Sasala Named Deputy Director for Army's Business Transformation Office," (February 2, 2023). ExecutiveGov, https://executivegov.com/2023/02/thomas-sasala-named-deputy-director-for-armys-business-transformation-office.
60. Jordan L. Fletcher and Eliahu H. Niewood, "Starting Simple with JADC2," (May 2023). MITRE, https://www.mitre.org/sites/default/files/2023-05/Starting_Simple_with_JADC2.pdf, 2
61. Artem Minaev, "The DAO Hack Explained: Understanding the Infamous Attack," (June 13, 2023). The CryptoDose Website, https://cryptodose.net/learn/the-dao-hack/.
62. David Siegel, "Understanding the DAO Attack," (updated January 13, 2023). The CoinDesk Company Website, https://www.coindesk.com/learn/understanding-the-dao-attack/.
63. Blockchains, Inc., "DAO.sol." (Accessed December 18, 2023). The Blockchains, Inc. GitHub Site, https://github.com/blockchainsllc/DAO/blob/6967d70e0e11762c1c34830d7ef2b86e62ff868e/DAO.sol#L747. Line 747.
64. Solidity Language Website. "Types – Solidity 0.8.21 Documentation," (Accessed September 5, 2024). The Ethereum Foundation, https://docs.soliditylang.org/en/v0.8.21/types.html.
65. 101st United States Congress, *Department of Defense Appropriations Act, 1991*, (November 5, 1990). Public Law 101-511, https://uscode.house.gov/statutes/pl/101/511.pdf., p. 41, Sec. 8092.
66. Ricky E. Sward, "The Rise, Fall and Persistence of Ada," (October 24, 2010). New York: Association for Computing Machinery (ACM) SIGAda Annual International Conference, Vol. 30, No. 3. https://doi.org/10.1145/1879097.1879081, 1.
67. The White House, "Back to Building Blocks: A Path Toward Secure and Measurable Software," (February 2024). https://www.whitehouse.gov/wp-content/uploads/2024/02/Final-ONCD-Technical-Report.pdf. 7.

Forward Persistence in Great Power Cyber Competition

Military Assets in a Relative Power Erosion Framework

Dr. Thomas F. Lynch III

ABSTRACT

The United States, the People's Republic of China (PRC), and Russia are engaged in strategic competition below the threshold of armed conflict. Cyberspace is its principal medium, and unless indicated otherwise, all references herein will assume the context of "short of armed conflict." America's relative power stature is under non-stop cyber duress from these rivals. Protecting America's three main peacetime power sinews – its economic edge; domestic political cohesion and electoral system confidence; and public trust in protection of personal privacy and security – from the subversive and corrosive cyber activities by Great Power rivals requires an array of U.S. government agencies, especially the U.S. military. The new era of Great Power strategic competition has fragmented the internet and rendered inadequate America's historical preference for an orderly, law-based framework that manages cyber-competition. The U.S. needs to focus on a Relative Power Erosion Framework featuring persistent engagement and a hunt forward posture. USCYBERCOM-led cyber campaigns are necessary in the short-term for effective American strategic cyber competition. In the longer-term, unique American military capabilities for persistent cyber engagement should be replaced with those in selected civilian governmental agencies more befitting of a 'new normal' for endemic cyber-competitive interactions among the Great Powers.

CONTEMPORARY GREAT POWER COMPETITION – THE ALTERED GEOSTRATEGIC ENVIRONMENT AND INTEGRATED DETERRENCE

Today's geostrategic environment is dominated by Great Power rivalry and competition for relative power gains and advantages among the U.S., Russia, and the PRC during cyber interactions.[1] This environment differs fundamentally from the previous geostrategic era. For almost thirty years, from the 1990s to the early 2010s,

Dr. Thomas F. Lynch III is a Distinguished Research Fellow in the Center for Strategic Research (CSR) at the Institute of National Strategic Studies (INSS) of the National Defense University (NDU) in Washington, D.C. His ongoing research primarily focuses on contemporary Great Power Competition and on India's strategic rise and implications for Indo-Pacific security and stability. He joined NDU in 2010 after retiring as a Colonel from a 28-year career in the active-duty U.S. Army, serving in a variety of command and staff positions as an armor/cavalry officer and as a senior level politico-military analyst. He holds a B.S. from the U.S. Military Academy at West Point, a Masters in Public Administration (MPA) and a Masters (M.A.) and Ph.D. in International Relations from the School of Public & International Affairs at Princeton University.

the U.S. was globally dominant. It's rules, norms, and preferences heavily shaped the evolution of global patterns, procedures, and protocols for most state-to-state interactions, including those in the new domain of cyberspace.[2]

The Reality of Strategic Competition in the Altered Geostrategic Environment

Cyberspace evolved and dramatically expanded worldwide in an open and liberal global environment with a unified, U.S.-preferred system that featured cooperative economic and social interactions. For most of this thirty-year, U.S.-dominated period, emerging Great Power rivals, the PRC and Russia, generally acted in accordance with these basic U.S. preferences.[3] Since the late 2000s, the PRC and Russia have remained engaged with the U.S.-normed global internet if beneficial, but increasingly are using it in coercive and confrontational ways: constraining outsider access, manipulating internal content, conducting industrial scale economic espionage and data collection, and manipulating rival state political and social discord for competitive strategic advantage.[4]

Putin's Russia, the weakest of the three Great Powers, has turned to cyberspace as its primary vehicle to reduce relative American ideological power and information dominance. Russia's approach to strategic cyber-manipulation echoes the "Active Measures" campaigns run by the U.S.S.R. against the U.S. during the Cold War but with vastly improved technologies and tactics.[5] Cyberspace access to the internet and social media's global openness allows Moscow to directly manipulate critical aspects of the U.S.'s dominant relative power in key strategic areas: *political legitimacy* and *personal privacy & security*.[6]

> Since at least 2008, the Russian state has directed coercive peacetime cyber campaigns aimed at weakening America's relative power in four major areas public confidence in the safety

of American critical infrastructure, the integrity of the American electoral system, the social stability of American society, and average American trust in their government.[7]

Russian military and intelligence services directly responsible for attacking the U.S. in these four areas include: the Russian Federal Security Service (FSB), including FSB's Center 16 and Center 18; the Russian Foreign Intelligence Service (SVR); the Russian General Staff Main Intelligence Directorate (GRU), 85th Main Special Service Center (GTsSS); GRU's Main Center for Special Technologies (GTsST); and the Russian Ministry of Defense, Central Scientific Institute of Chemistry and Mechanics (TsNIIKhM). The FSB has conducted malicious cyber operations targeting U.K. and U.S. energy companies, U.S. aviation organizations, U.S. government and military personnel, private organizations, cybersecurity companies, and journalists. The GRU has organized special military units to politically interfere in the U.S. and other western democracies. GRU Military Units 26265 and 74455 led the 2016 hack into Democratic National Committee computer systems. Unit 26265 developed the malicious software for that penetrated and Unit 74455 assisted in disseminating stolen documents and anti-Clinton narratives to online personas like DCLeaks and Guccifer 2.0. Unit 74455 also hacked into computers at U.S. state boards of elections and companies supplying election technologies.[8] Russian cyber interference in U.S. national elections continued into the 2024 cycle with a widening array of sophisticated online and social media influence campaigns exposed by the U.S. Justice Department with a public announcement of interference indictments in September 2024.[9]

Russian security agencies are also covertly tied to an array of domestic and international cyber ransomware and economic espionage groups that are gradually degrading American political comity, social cohesion, and confidence in its monetary and financial system. Russian state-sponsored cyber actors have demonstrated capabilities that compromise information technology (IT) networks, maintain long-term, persistent access to IT networks, extract sensitive data from IT and operational technology (OT) networks, and disrupt critical industrial control systems (ICS)/OT functions by deploying destructive malware. The FSB also contracts criminal hackers for espionage-focused cyber activity, hackers that separately have launched disruptive ransomware and phishing campaigns.[10] Moscow provides sanctuary and protection to all of its state-controlled group members and most of its affiliated hacker groups, making fear of criminal indictment or international sanction a non-factor insofar as deterrence.

The PRC has competed since at least 2008 to improve relative strategic power vis-à-vis the U.S. by eroding Washington's status, stature, and innate advantages by targeting three primary areas:

- America's relative economic wealth and security;
- Trust and confidence in the U.S.'s ability to protect sensitive and private personal data (PII) from exploitation;
- America's international political legitimacy.

In early 2024, U.S. intelligence agencies and journalists reported that the PRC – applying

practices honed by Russian cyber-actors – were conducting an array of cyberspace misinformation and deception activities to influence the U.S. Presidential elections.[11] In September 2024, the U.S. research company Graphika demonstrated that a Chinese-linked cyber and social media campaign dubbed "Dragonbridge" had been impersonating U.S. voters while denigrating U.S. politicians and circulating false messages.[12] This report and subsequent U.S. government confirmation reflected the PRC's growing resolve to conduct cyber campaigns that *erode the sanctity of the American electoral system*. Revelations during 2024 confirmed that the PRC's cyber-competitive efforts against the U.S. have been growing in the political space. However, Beijing's primary malign cyber activity remains focused *on enhancing China's relative economic wealth*. The PRC's current cyber operations can be characterized as controlling information at home and stealing secrets abroad.[13]

For decades, the PRC has pursued a deliberate cyber espionage campaign against American firms and their partners both in China and abroad, focusing on the brazen theft of intellectual property and other sensitive commercial data and processes. PRC cyber campaigns include groups operating within the structure of the Chinese military and intelligence services and many People's Liberation Army (PLA) units (e.g., PLA Units 61398 and 78020). They also feature an array of PRC-affiliated private cyber espionage groups known as Advanced Persistent Threat (APT) entities like APT 41 (Double Dragon) and a host of others.

Leading cybersecurity analysts like James Lewis of the Center for Strategic and International Studies (CSIS) estimate that the U.S. lost between $20 – $30 billion annually from 2000 – 2017 and a cumulative total of $600 billion over the period as the result of the PRC's economic tradecraft, marketing practices, and intellectual property (IP) cyber theft.[14] The downstream economic multiplier impacts from IP cyber theft in lost markets and employment opportunities across the global marketplace drive this number much higher – and likely to more than $50 billion annually.[15] Estimates that explicitly incorporate PRC gains from counterfeited goods, in addition to IP theft, peg annual U.S. economic losses even higher – in a range between $225 billion to $600 billion.[16] Limited to pirated IP and put in context of the relative trajectory of the Sino-American Great Power economic rivalry, The World Bank estimated that the U.S. GDP in 2010 was $15 trillion, moving to $21 trillion in 2020, and Chinese GDP was $6 trillion in 2010, expanding to $14.75 trillion in 2020, a relative gain of approximately 30 percent. Other factors contributed to this relative wealth gain, but more than two decades of PRC cyber theft explains a non-trivial portion of Beijing's significant growth in strategic economic power vis-à-vis the United States.[17]

Malicious PRC cyber activities target a variety of U.S. industries, agencies and organizations including: healthcare, financial services, defense industrial base, energy, government facilities, chemical, critical manufacturing (including automotive and aerospace), communications, IT (including managed service providers), international trade, education, video gaming, faith-based organizations, and law firms. PRC state-sponsored cyber actors aggressively target military, educational, and critical infrastructure (CI) personnel and organizations to

steal sensitive data, critical and emerging key technologies, intellectual property, and personally identifiable information (PII). Some target sectors include managed service providers, semiconductor companies, the Defense Industrial Base (DIB), universities, and medical institutions. These cyber operations support the PRC's long-term economic and military development objectives.[18] Like Moscow, Beijing affords broad sanctuary and protection to the members of its state-controlled group members and private hacker agents and will not extradite them. This sanctuary explains why the U.S. Department of Justice (DoJ) and the FBI have indicted dozens of Chinese state hackers but there have been no noteworthy apprehensions or prosecutions and no measurable alteration in malevolent Chinese cyber-behavior. Because of the fundamentally altered geostrategic power structure, Chinese hackers have little fear from criminal indictment or meaningful sanction by traditional U.S. or international legal and law enforcement activities.[19]

This fragmentation of cyberspace with the return of Great Power rivalry and the use of cyber for strategically significant competition is consistent with the history of fragmentation and separation of global domains of state-to-state interaction under growing geostrategic duress. As with the electronic warfare (EW) and the air domains before it, the cyber domain promises to continue a trajectory of increasing fragmentation until a major geostrategic shock – like an armed conflict between the Great Powers – re-frames global power relationships in a manner enabling return to a more cooperative and collaborative norm.[20] Clint Watts, an American cyberspace analyst, noted the world is now comprised of three distinct cyber domains: a highly manipulated and coercive one preferred by Russia, a tightly constrained, mostly closed, self-interested one preferred by the PRC, and an open and free one preferred by the U.S. and its partners.[21] A U.S. Council on Foreign Relations report from mid-2022 concluded that the competition for internet data in cyberspace is the primary dynamic of Great Power strategic competition and is responsible for accelerating cyberspace fragmentation that will not be reversed.[22]

The Waning Relevance of a Legal/Law Enforcement Framework for Competing in Cyberspace

Despite the relative comity and cooperation just after the advent of the internet, the international arena has yet to develop enforceable legal standards that govern acceptable conduct in cyberspace. Even during the 1990s and early 2000s, the level of distrust among major states was too high to conceive of a legally binding multi-state cyber treaty. Alternative efforts to generate a set of nonbinding norms and confidence-building measures (CBMs) produced a 2010 U.N. Report with five recommendations for negotiating safety and security in international cyberspace, but without follow-on success.[23] The ambitious collective effort that resulted in the *Tallinn 2.0 Manual on the International Law Applicable to Cyber Operations* (2017) was a forward-looking effort to grope with applying international law to cyberspace operations. But this non-legally binding academic manual by western legal scholars and cyber analysts has yet to gain universal policy traction.[24] There remains an imperative for the U.S. to stand with like-minded allies on commitment to a single, interconnected cyber system for all of humanity

that fosters innovation, economic growth, creativity, democratic governance, and unfettered access to knowledge. At least within this group, the U.S. may be able to collectively frame and enforce norms against destructive cyber-attacks and coercive cyber campaigns designed for strategically significant power erosion of state rivals.[25]

And within this network, institutions and protocols can be enhanced and extended under an agreed framework that effectively sanctions private and government-sponsored criminal or destructive activities. American legal and law enforcement traditions for safeguarding strategically critical economic, political, and social functions can continue within this collaborative cyber network. The Department of Homeland Security, the DoJ, and the FBI partnering with the Department of State and the CIA – with improved funding and cyber-tools – can pursue warrants, apprehension, standards of evidence, and traditional means for bringing to justice those threatening the norms and laws governing a free and responsible internet.[26]

However, the perverse and persistent use of cyberspace against America and its allies by Russian and PRC state-run and state-protected malevolent actors seeking strategic advantage over time is not today – and cannot for the foreseeable future be – optimally managed by legal and law enforcement traditions and protocols. Specifically, Russian and PRC refusal to extradite those indicted for abusive cyber behavior has been consistently demonstrated for almost a decade. At the end 2021, there had been no major apprehensions of the indicted, no trials, and no significant indication that malevolent cyber intentions or behaviors have been altered nor were there any growing public and private concerns about the effectiveness of indictments as a tool of deterrence.[27] In late 2024, no compelling information exists to attenuate these concerns. Effective sanctuary for these persistent cyber actors seeking the long-term erosion of American power renders them untouchable by ethically won legal indictments or national sanctions. In addition, evidence from Russia indicates that cyber-entrepreneurialism and experimentation continue to thrive in a sanctions-constrained, and indictment-ladened environment at least in part because Russian government and private-sector ties are tightening.[28] Legal frameworks and law enforcement protocols against Great Power actors remains necessary, but a different framework for effective competition in cyberspace is required.

The Growing Importance of a Relative Power Erosion Framework for Competing in Cyberspace

Indictments and sanctions of foreign cybercriminals remains necessary for consistent application of cyber-norms, but alone are insufficient insofar as meaningful deterrence or disruption of adversary Great Power cyber organizations and their affiliates. A necessary and sufficient framework is required – one that better aligns with the realities of a fragmenting and strategically abused cyberspace.

An era of strategic Great Power competition requires a more holistic and aggressive approach

to blunt rival cyber activities that erode American power, bleed American economic wealth and know-how, compromise major American interests, or corrode American political and social cohesion. Multiple American agencies should participate in strategic competition in cyberspace given that the cyber domain has fragmented and the threat from America's cyber rivals require a different competitive framework.

Competition with America's Great Power rivals requires a ***Relative Power Erosion Framework*** in response to the increasingly fragmented cyber domain and its unique nature. In turn this ***Relative Power Erosion Framework*** rests comfortably on the foundational logic of persistence-as-deterrence in cyberspace, or **cyber persistence theory**.[29]

The **cyber persistence theory** construct derives from the cyber-strategic environment, which differs from conventional and nuclear deterrence, and requires continuous interaction, cumulative strategic effect, ***persistent engagement***, and ***forward defense***.[30] **Cyber persistence theory** views as normal certain occurrences that would be failures in other domains. Cyber aggression, rather than an anomaly, signals emergence of a new competitive space wherein "agreement over the substantive character of acceptable and unacceptable behaviors ... is currently immature," thereby recasting what is "normal."[31]

Classic deterrence theory – with its core concepts of denial, cost imposition, signaling, and attacks of significant consequence – now sits side-by-side with a paradigm/construct more aptly tailored to the cyber environment: ***cyber persistence***. Cyber persistence features continuous interaction, cumulative strategic effect, persistent engagement, and forward defense.[32] The core question for the cyber persistence paradigm is how to secure when you cannot deter.

Since just after the mid-2000s, deterrence in cyberspace has been contrasted from classic military deterrence and nuclear weapons deterrence. A renowned RAND study from this era described cyberspace as a unique medium of global interaction with its own rules, with attacks enabled through the exploitation of vulnerabilities instead of force, where permanent effects are harder to produce. It also is a medium fraught with ambiguities about who attacked, why, what they achieved and whether they can do so again even if – and often because – of successful attacks.[33]

Throughout the 2010s and into the 2020s, the limitations of deterrence formulations in cyberspace have been intensely debated. Increasingly, prominent analysts argue that traditional deterrence constructs are less relevant in cyberspace, and that a new construct was needed.[34] Others, including Harvard political scientist Joseph Nye, have argued that classic deterrence thinking has utility in cyberspace, but that this thinking must be "stretched" logically and creatively to move beyond it,[35] and preventing harm in cyberspace involves four formal mechanisms: denial, punishment, entanglement and norms.[36]

By the end of the 2010s, most experts on cyber-theory began to coalesce around a consensus

that classic deterrence premises ill-fitted to challenges in cyberspace. Deterrence theory's core concepts of denial, cost imposition, signaling and discrete attacks of major strategic consequence would not accurately address the emerging pattern of coercive Great Power interactions in cyberspace, with the exception of cyber interactions in the context of armed conflict, especially those triggering nuclear weapons. At all other times during rivalrous state-to-state activities involving strategic competition, confrontation, and other crisis management, the unique interdependences of cyberspace and the inherent challenges of attributing malevolent activities undermined the efficacy of deterrence by punishment or denial, and made a mockery of deterrence by entanglement. The bulk of cyberspace exchanges featured concepts of continuous interaction, cumulative strategic effect, persistent engagement, and forward defense. Cyber competition expert Emily Goldman put it this way in a 2020 book chapter on the topic,

> ... the frustration (crisis) was not that deterrence was not working at all but that it was not stopping the burgeoning numbers of attacks below the threshold of armed conflict and that these attacks cumulatively were leading to relative power loss. Deterrence arguably has been effective in the cyber strategic space of armed conflict. States, it would appear, are choosing to abide by conventions codified in United Nations Charter articles 2(4) and 51, which speak to the use of force and the right of self-defense in the event of armed attack. They also recognize that the United States can respond across domains (using its advantages) to a cyber-attack should they violate those conventions. The failures have been in assuming that deterrence would also be successful in the strategic space short of armed conflict, and, more fundamentally, in not understanding that those two strategic spaces even existed. Decision makers needed a paradigm shift to recognize the existence of distinct strategic spaces that had opened a seam in great power competition that in turn others were exploiting, to explain why this dynamic came about, and to offer a new strategy better aligned to cyberspace's structural and operational imperatives.[37]

The core challenge for deterrence and cyberspace is one of how to deter cyberattacks when they cannot be defended against and when attribution is ambiguous. Dr. Goldman and kindred cyberspace experts posited the existence of a new framework for securing strategic national interests in cyberspace: cyber-persistence theory. Persistence theory asks how to secure when you cannot deter.[38]

The **cyber persistence theory** paradigm does not deny the viability of deterrence in cyberspace. Indeed, the persistence paradigm agrees that classic framing of deterrence theory has applicability, but only if applied in enlightened and extended ways.[39] ***Cyber persistence theory*** restricts historic definitions of deterrence to where they logically reside – during cyber operations paired with armed attacks or equivalent to armed attacks. Persistence theory eschews overarching focus on specific "significant cyber incidents." Instead, it asserts that the realities of cyberspace mean that constant contact between rivals is omnipresent and

where "strategic significance" happens not as the result of any single event but rather emerges from the cumulative effect of a coercive cyber campaign compromising many individually less consequential operations carried out towards a coherent strategic end.[40]

Cyber persistence theory comports well with the realities of Great Power strategic competition where cumulative strategic effects can matter even more to relative power gains and losses than the risks from any one destructive cyber act. As American cyber expert James Lewis wrote recently,

> The most damaging cyber incidents are actions by states as part of some larger interstate confrontation or conflict. We will only see physical destruction and casualties from cyber operations when they are part of some larger armed conflict...This is important because, in the absence of the risk of significant damage that armed conflict brings, there is little incentive for states with offensive cyber capabilities to make concessions in their use, much less agree to disarm.[41]

Grounded in **cyber persistence theory**, a ***Relative Power Erosion Framework*** for successful Great Power Competition understands cyberspace that is micro-vulnerable but macro-resilient. The contested, fragmenting cyber domain is inherently exploitable but simultaneously stable in that states are unlikely to sustain a knock-out blow from a peacetime cyber-strike alone. Great Powers also are disinclined to escalate from cyber exchanges to armed conflict because the strategic risks from such escalation are infinitely more destructive and worrisome than those found alone in the cyber domain. Analysts who fear triggering armed conflict from persistent cyber operations and activities face a burden of proof that has not yet been evident in the cyber domain.[42]

Integrated Deterrence and Cyber Campaigning: Cyber Persistence and Hunt Forward

Cyberspace already features Great Power strategic campaigning - Russia and the PRC strategic cyber campaigns, often leveraging private hackers and criminals in addition to national security, intelligence, and military organizations and their operatives, for more than a decade. Meaningful consequences to these coercive strategic cyberspace activities by America's Great Power rivals has been too low. Although attribution of PRC and Russian strategic cyber coercion has improved over the past decade, the U.S. remains bereft of any meaningful ability to: remove options and opportunities for this coercion, create significant friction in their coercion attempts, or threaten them with credible and meaningful responses.[43]

It took Washington until 2018 to recognize the serious consequences from persistent strategic competition in the cyber domain. It then generated a limited, targeted, but credible response by endowing USCYBERCOM and the NSA with necessary authorities to protect the sanctity of U.S. national elections from external cyber-enabled manipulation and disruption. The USCYBERCOM-NSA strategy to counter strategic cyber-rivalry featured the twinned concepts of "persistent cyber engagement" and "hunt forward."[44]

USCYBERCOM and NSA's pursuit of persistent cyber engagement with forward-deployed hunt forward teams was unique in 2018 and remains so today. Working with U.S. partners and allies, hunt forward teams establish attribution and identify means and mechanisms involved in adversarial cyber campaigns that are far more than discrete malicious cyber activities. Forward USCYBERCOM teams integrate offensive and defensive operations to attain and maintain a cyberspace superiority over rivals conducting coercive cyber campaigns. Hunt forward teams are equipped for counter- cyber missions that can disrupt, negate, and/or destroy adversarial cyberspace activities and capabilities, both before and after their employment.[45]

The 2022 National Defense Strategy (NDS) Fact Sheet focuses on "integrated deterrence" as one of three primary ways that the Department of Defense (DoD) will advance national goals against its major rivals in the new era of Great Power Competition. It calls for developing and combining DoD strengths with other elements of national and international partner power across all warfighting domains and the spectrum of conflict.[46] Implicit in the "integrated deterrence" construct is that DoD must possess cyber assets with comparative advantages over those found in other government or private entities; thus, DoD cyber assets can be used effectively and efficiently across the range of strategically competitive activities with American Great Power rivals including those below the threshold of armed conflict.[47]

Integrated deterrence has been discussed during 2021 – 2022 as an effort in the modern era for the United States to frame deterrence across a number of different conceptual categories: the many domains of state-to-state interaction, *the broad spectrum of conflict*; all the instruments of national power, and with allies and partner states. Proponents suggest that modern era deterrence be integrated across multiple domains: conventional, nuclear, space, and cyber. They seek deterrence in these domains across an integrated spectrum of conflict from "high end" nuclear weapons conflict, conventional weapons conflict, and into the hybrid or gray zone spectrum of conflict where non-kinetic weapons and irregular tactics are utilized. They seek deterrence that is integrated across all instruments of national power – not just military – to dissuade would-be aggression including: military, diplomatic, economic, social, cultural, and information. They also aspire that integrated deterrence be constructed in a framework engaging allies and partner states in the processes.

The U.S. Cyberspace Solarium Commission Report of early 2020 recommended a national cyber strategy of ***layered cyber deterrence***.[48] Layered cyber deterrence aims in three ways to lower – not eliminate – the probability and adverse consequences of cyberattacks. The first is to deny benefits to cyber attackers by securing critical networks in a public-private partnership that promotes network security and national resilience. The second is to impose costs and the third deterrence layer is to shape behavior. Costs and shaping both require network ***persistence*** – the constant engagement and interaction of cyber entities across the international cyber environment.[49]

The 2022 NDS identifies "campaigning" as a critical component of DoD activity and aligns three DoD campaigning activities with other instruments of national power: (1) undermining acute forms of competitor coercion, (2) complicating competitor military preparations, and (3) developing/testing warfighting capabilities with allies and partners.[50]

Persistent Cyber Operations featuring ***hunt forward*** teams is fully consistent with the construct of layered cyber deterrence and strategic campaigning. Thus, a ***Relative Power Erosion Framework*** featuring *persistent engagement* and *hunt forward* USCYBERCOM teams should be key features of U.S. national integrated deterrence.

Whenever Cyber Persistence or defending forward conflates or even overlaps with offense, the legitimately defensive role inherent played by persistent engagement is imperiled. Objections to escalation and escalation dominance presuppose a spiraling interaction dynamic that inevitably leads offensive cyber operations to armed conflict. Yet contemporary academic literature views persistent cyber engagement, and even some offensive cyber activities as non-violent alternatives to conventional armed conflict, and hence less escalatory than activities involving conventional or nuclear weapons.[51] Moreover, focus upon "significant cyber incidents" traces back to the *model of episodic contact* dominant in nuclear and conventional deterrence.[52] "Strategic significance" in cyberspace seldom results from a single event, but rather, from the cumulative effect of a deliberate campaign comprising many individual operations/activities carried out toward a coherent strategic end.[53] None of the known cases of proactive, defend forward strategic cyber operations conducted against rival state-run or state-sponsored malicious cyber actors since 2018 have provoked dangerous escalation dynamics.[54] Thus, the burden of proof is on those concerned that offensive cyber actions could dangerously escalate, not the other way around.

THE WAY AHEAD FOR USCYBERCOM IN GREAT POWER COMPETITION

In the cyber-environment, as in all domains of state-to-state interactions, Great Power rivals compete over three strategic "prizes:" (1) intellectual property that contributes to how innovation occurs and how wealth is generated; (2) legitimacy – political and social; and (3) privacy of personal information.[55]

Cyberspace is a domain of economic, diplomatic, informational, and military interaction and persistent, integrated Great Power campaigns up to the very brink of armed conflict. Well before crises arise, robust cyberspace campaigns and counter-campaigns, must integrate the best government-wide and private sector tools, techniques and procedures and thereby deter. At the same time if deterrence fails, the ability to counter adversaries that opt for kinetic warfare remains an ongoing imperative.[56] The construct of campaigning lends itself inherently to incorporation of key U.S. military cyber assets – especially those uniquely well-developed already for "hunt forward" and "cyber persistence" into the competitive framework of cyber activities amongst and between America and its Great Power rivals.

Beginning in the early 2010s, and accelerating over the past half-decade, USCYBERCOM has been granted limited and important authorizations to conduct non-combat, persistent cyber offensive operations.[57] Since at least 2017, the USCYBERCOM-NSA nexus reportedly has participated in limited, time-constrained persistent engagement peacetime operations from forward locations – operations that penetrate, exploit data, disrupt, or retaliate against rival non-state groups (like ISIS) and hostile states (e.g., Russia and Iran), and others that threaten the U.S., our allies, or major global security and sovereignty norms.[58]

Over the past decade, and especially since 2017/2018, USCYBERCOM has shifted from a response force focused on defending DoD networks and supporting counterterrorism and conventional force activities, to one featuring ***persistent engagement***. Since its March 2018 vision document, USCYBERCOM has featured a strategic concept of ***cyber persistence***, recognizing that successful Great Power Competition requires actively contesting and confronting adversary efforts to enhance relative power and achieve decisive strategic outcomes from cumulative tactical impacts in cyberspace.[59] To meet this challenge, USCYBERCOM must operate continuously both *forward* – in physical and virtual realms – and at increasing scale. Thus, the 2018 cyber-strategic command vision formalizes a framework for operations to secure U.S. cyberspace by influencing and shaping adversary behavior through ***Persistent and Integrated Forward Engagement***.[60]

In adopting ***Persistent Forward Engagement***, USCYBERCOM acknowledged that deterrence of adversary malevolent actions *within the cyberspace domain*, while feasible, requires a different kind of operational framework.[61] Helpfully, the FY2019 National Defense Authorization Act (NDAA) designated cyber reconnaissance and surveillance as a traditional military activity – providing enhanced authority for offensive cyber operations in campaign planning and responses to malign adversary activities.[62]

USCYBERCOM military units and procedures have provided vital and unreplaceable support to U.S. civilian authorities and agencies in a number of campaigns including ones in Montenegro that improved American cyber defenses ahead of the 2020 elections and ongoing actions from forward locations to inoculate the U.S. and our allies from the persistent threat from Russian cyber actors and their proxies supporting war against Ukraine.[63]

Together, the limited USCYBERCOM campaigns have achieved critical competitive objectives in the following strategically significant categories:

- Disrupt Russian foreign influence operations in cyberspace targeting U.S. and western elections;
- Disrupt or degrade Russian and PRC economic espionage operations;
- Deter, disrupt, or degrade Russian (and Iranian) cut-out and proxy cyber operations targeting U.S. critical infrastructure;

- Identify and publicly attribute cyberattack malware by the so-called MuddyWater Group to Iranian Intelligence Services (MOIS) actively used to siphon data from government and telecom firms across the Middle East, publishing the code it used to alert improved cyber defense.[64]

The open question is how best to extend/expand the legal, ethical, and effective reach of U.S. military cyber campaigns and operations during times of competition and confrontation. As it was when General Keith Alexander testified before Congress in 2010, there remains much uncharted territory in the world of cyber policy, law, and doctrine.[65] But the historical record of military participation in strategic competition and the recent successes of USCYBERCOM campaigns and operations safeguarding vital American relative power in a peacetime environment both validate the legitimacy of greater military cyber participation in cyber campaigns – at least for a period of time.

The 'dual hat' USCYBERCOM-NSA command relationship already appears optimized to assure the agile and responsive interface between cyber-intelligence and cyber-operations against strategic rivals below the threshold of armed conflict.[66] The proper orientation and appropriate resourcing of USCYBERCOM to scale for these critical cyber campaigns requires greater American policy maker attention. To be successful at the appropriate scale, expanded national investment in cyber national mission teams and a more detailed legislative agenda establishing the legal and bureaucratic authorities for military-led, cyber persistence activities is necessary.[67]

Retaining the USCYBERCOM-NSA Dual Hat

The USCYBERCOM-NSA tight coupling and shared "dual hat" command structure establishes many vital interactions for successful strategic cyber-competition with America's Great Power adversaries.[68] Among these critical synergies are the three identified frequently by former USCYBERCOM Commander, General Paul Nakasone: "..speed, agility, and a unity of action between world class code-makers and code-breakers."[69] Unique among USG agencies and agency-teams, USCYBERCOM today alone can operate in cyberspace outside the U.S. against adversaries before they can do great harm inside the United States. USCYBERCOM can establish "persistent engagement" while "defending forward" in cyberspace with partners and allies that help attribute malicious actors, disrupt their activities before they strike, and impose costs on them that make it difficult to operate in space and time against strategically significant elements of national power.[70] The USCYBERCOM-NSA "dual hat" has stirred debate since USCYBERCOM was established in 2010, and numerous reviews and studies have been done about this peculiar relationship with an eye to separating them when appropriate. A 2023 report led by former Chairman of the Joint Staff, General Joseph Dunford, determined that retaining the "dual hat" for the foreseeable future was a net positive for national security.[71]

Retaining the "dual hat" aligns with geopolitical realities for cyberspace in this new era of multi-polar Great Power competition. Other key USG sectors need to build-out credible and responsible defensive, offensive, and enabling cyber tools to compete with rival state exploitation of cyberspace for decisive strategic advantage. But today, the dynamics of an intensifying multi-state Great Power Competition warn against under-utilizing the well-developed "hunt forward" and "persistent engagement" capabilities now found almost uniquely in the USCYBERCOM-NSA nexus. Managed in accordance with liberal and democratic values, the use of USCYBERCOM event-tested cyber ***hunt forward*** teams and ***persistent engagement*** strategies must be enabled and resourced for some reasonable transition period – likely through the end of the 2020s – if the U.S. is to stem the erosion of its relative power in critical areas before they compound into negative strategic impact.[72]

Expanding (Temporarily) Cyber Mission Force (CMF) Teams for Vital Strategic Competition

USCYBERCOM's 2018 vision argues that, at least for a period of time, U.S. whole of government capabilities and processes remain insufficient and destined to keep the U.S. in a reactive mode after costly intrusions or attacks occur into America's cyber critical infrastructure, and that DoD is the leader (at least for now) in building the operational expertise and capacity to meet critical cyberspace threats and stop cyber aggression before it can be used by our rivals to secure strategic advantage.[73] This analysis remains accurate in 2024, yet more capacity is needed to provide options and capabilities to conduct strategically significant cyber competition throughout times of peace and up to the brink of actual armed conflict.[74]

The USCYBERCOM-NSA nexus remains the right locus for expanding capacity for strategically significant cyber competition.[75] But this expansion needs be prudent, constrained, and properly resourced and authorized by Congress and the White House.

As of early 2024, USCYBERCOM had just 133 Cyber Mission Force (CMF) teams with varying cyber-operational mission sets.[76] Only some of these are organized for the important ***hunt forward*** missions capable of assuring persistent engagement in partnership with U.S. international partners and allies. The number of CMF teams is programmed to grow to 147 by late 2024, but even at this expanded number, CMF teams could not undertake a vast array of missions required to contest single-event or stochastic ransomware, denial of service attacks, or espionage activities across the national economic, political, social and personal privacy dimensions of cyberspace.[77] Not all cyber-attacks against America and its allies are strategic in nature despite the understandable concerns felt by their victims.[78] Instead, the USG requires a more robust and durable capability to conduct persistent engagement and hunt forward missions aimed against the deliberate cyber campaigns undertaken by Great Power rivals China and Russia. The legitimate targets of these American cyber campaigns should include state-based cyber actors and state-affiliated ones credibly tied to these Great Power competitor state strategic cyber-campaigns.

Additional CMF teams should be resourced and USCYBERCOM-NSA given Congressional enabling authorities to develop and execute cyber campaign and counter-cyber campaign plans that pursue state and non-state actors credibly deemed culpable of conducting cyber campaigns directed by or coordinated with the PRC or Russia to achieve strategic cumulative effects against the U.S. or allies in the following vital areas of national power:

- Relative economic advantage through industrial espionage or via disruption and degradation of US productivity;
- Political confidence and social cohesion by manipulating the U.S. elections processes;
- Citizen confidence and trust in the U.S. government's ability to safeguard the privacy and personal security of citizens.

USCYBERCOM should be appropriately resourced for growth to 200 total CMF teams over the course of the 2025-2030 Future Years' Defense Program (FYDP 25-30). The NSA budget should be enhanced in parallel to build-out the support structure for these teams. This growth should allow for USCYBERCOM to generate forward presence by an additional 25-30 ***hunt forward*** teams at any given time with explicit focus on campaigns aimed at Russia and the PRC and in the three areas of national strategic competition.

Military-led cyber campaigns are a short-term necessity but not optimal for the long haul. As Great Power Competition continues to evolve, expedient and necessary use of military cyber capabilities to conduct persistent cyber engagement should be replaced with capabilities within the civilian governmental structure that is befitting of a 'new normal' of endemic competitive relations between the Great Powers.

Congress and the Executive should push the following government organizations to generate their own CMF-style ***hunt forward*** teams with appropriate funding and authorities to take the lead on cyber campaigns by the early 2030s: Department of Homeland Security (DHS), Department of State (DoS), Department of Justice (DoJ), Department of Commerce (DoC), and the FBI. The *Cyberspace Solarium Commission Report* of 2020 calls for expansion of the concept of "defend forward" across the government built on the concept originated in the Department of Defense but using all instruments of national power.[78] Empowering hunt forward teams in these agencies would enhance America's competitive ability to disrupt and defeat growing adversary cyber campaigns across an array of threat vectors. The U.S. *National Cybersecurity Strategy* of March 2023 also establishes this as a necessary part of the U.S. government's strategic objective to integrate federal cyber disruption activities, but it also notes that upgrading and properly organizing this will take time.[80] So for now, USCYBERCOM-NSA cyber persistence and disruptive capabilities are the best we have. The longer-term process of federal integration should include provisions for a cross-leveling of individuals and resources from the new USCYBERCOM CMFs to the interagency team analogs with an aim of drawing back USCYBERCOM CMF teams to around 150 as the interagency brings some 50 or so teams into fully operational status during the 2030s.[81]

CONCLUSIONS

America's once dominant geostrategic position has measurably diminished. Today we find ourselves in an evolving era of Great Power Competition. Also seriously under threat is America's longstanding dominance in cyberspace. Where American ascendance in cyber hardware, software, infrastructure design, and norms for appropriate use in a one-world cooperative framework once ruled supreme, today's cyber domain is characterized by increasing fragmentation, a drift into confrontational and coercive activities by one state against many others, and a preference by Russia and the PRC – America's Great Power rivals – to use cyberspace for aggressive campaigns that seek relative power gains against the U.S. and its allies in strategic competition.

Although it may be pursued among contemporary allies and partners, *a legal/law enforcement framework* for Great Power strategic competition in cyberspace is not sufficient in the face of durable cyber domain fragmentation. Instead, the U.S. must pursue a ***Relative Power Erosion Framework***, which requires use of all elements of U.S. national power. A ***Relative Power Erosion Framework*** for strategic competition in cyberspace aligns well with the new **cyber persistence theory**, and USCYBERCOM's ***persistent cyber engagement*** conducted by ***hunt forward*** military cyber teams.

A ***Relative Power Erosion Framewor***k featuring military cyber teams must be disciplined and focused on truly strategic cyber campaigns (and counter cyber campaigns) designed against Russian and Chinese cyber organizations and affiliated cyber actors conducting cyber campaigns aimed at one of three relative strategic gains:

- ***Relative economic advantage*** through espionage, disruption and degradation.
- Reduced ***domestic political cohesion, confidence and trust in the electoral system***; and
- Reduced faith and confidence in the U.S. being able to protect its citizens from coercive cyber campaigns that compromise ***privacy and personal security***.

A ***Relative Power Erosion Framework*** should feature USCYBERCOM CMF teams for a period of time limited to the end of the 2020s. By 2030, the U.S. should establish civilian interagency teams that operate as the military CMF teams operate today and thus take full control of persistent cyber engagements and hunt forward campaigns. The military-to-civilian transition for these peacetime cyber campaigns will help signal the necessary change in mindset by the entire U.S. government from one mistakenly assuming cyber cooperation to one properly structured for persistent and effective cyber competition.

DISCLAIMER

The views expressed in this article are those of the author and do not reflect the official policy or position of the United States Military Academy, The National Defense University, the Department of the Army, the Department of Defense, or the U.S. Government.

NOTES

1. Thomas F Lynch III ed., *Strategic Assessment 2020: Into a New Era of Great Power Competition*, (2020). Washington, D.C.: National Defense University (NDU) Washington, D.C.: National Defense University (NDU) Press, https://ndupress.ndu.edu/Portals/68/Documents/Books/SA2020/Strategic-Assessment-2020.pdf/, 59-65; Ali Wyne, *America's Great Power Opportunity: Revitalizing U.S. Foreign Policy to Meet the Challenges of Strategic Competition*, (July 5, 2022). Boston, MA: Polity Press, 45-65.
2. "ICANN's Historical Relationship with the U.S. Government," ICANN.org, last accessed, September 30, 2024, https://www.icann.org/en/history/icann-usg; Lynch ed., *Strategic Assessment 2020*, 46-59.
3. Lynch ed., *Strategic Assessment 2020*, 46-59
4. Dave Aitel, Sophia d'Antoine, Thomas Garwin, Ian Roos, Nicholas Rostow, Justin Sherman, and Abraham Wagner, (2022). *China's Cyber Operations: A Rising Threat to American National Security*, New York: Margin Research LLC for DARPA, 8-37; Dave Aitel, Sophia d'Antoine, Thomas Garwin, Ian Roos, Nicholas Rostow, Justin Sherman, and Abraham Wagner, (2022), *Russia's Cyber Operations: A Rising Threat to American National Security*, New York: Margin Research LLC for DARPA, 1-18, 49-82.
5. Fletcher Schoen and Christopher J. Lamb, Deception, *Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, (2012). NDU-INSS Strategic Perspectives 11, Washington, D.C.: NDU-Press; Dave Aitel, et al., *Russia's Cyber Operations*, 1-18, 49-82.
6. Scott Jasper, *Russian Cyber Operations: Coding the Boundaries of Conflict, (2020). Washington, D.C.: Georgetown University Press; Justin Sherman, Untangling the Russian web: Spies, proxies, and spectrums of Russian cyber behavior*, (September 19, 2022). Washington, D.C.: Atlantic Council, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/untangling-the-russian-web/.
7. Thomas F. Lynch, III, "The Future of Great Power Competition: Trajectories, Transitions, and Prospects for Catastrophic War," (July 25, 2024). *Joint Forces Quarterly*, Volume 114, 3rd Quarter, Washington, D.C.: NDU Press, https://digital-commons.ndu.edu/joint-force-quarterly/vol114/iss2/4/, 18; U.S. Department of Defense, *Summary – 2023 Cyber Strategy of the Department of Defense*, (September 2023). Washington, D.C:, https://www.defense.gov/News/Releases/Release/Article/3523199/dod-releases-2023-cyber-strategy-summary/, 4-5.
8. Dave Aitel, et al., *Russia's Cyber Operations*, 1-18, 49-82.
9. U.S. Department of Justice, *Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere*, (September 4, 2024). Washington, D.C., https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence; Shanon Bond, "Microsoft says Russia's election interference efforts have pivoted to Harris and Walz," (September 17, 2024). *NPR.org*, https://www.npr.org/2024/09/17/nx-s1-5116267/russia-election-interference-harris-walz-microsoft.
10. Cybersecurity and Infrastructure Security Agency (CISA), "Alert AA22-110A: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure," (last revised May 9, 2022). https://www.cisa.gov/uscert/ncas/alerts/aa22-110a; Dave Aitel, et al., *Russia's Cyber Operations*, 1-18, 49-82.
11. Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community – 2024*, (February 2024). https://www.odni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf, 12; Tiffany Hsu and Steven Lee Myers, "China's Advancing Efforts to Influence the U.S. Election Raise Alarms," (April 2, 2024). *The New York Times*, https://www.nytimes.com/2024/04/01/business/media/china-online-disinformation-us-election.html
12. Christopher Bing and Katie Paul, "US voters targeted by Chinese influence online, researchers say," (September 3, 2024). Reuters.com, https://www.reuters.com/world/us/us-voters-targeted-by-chinese-influence-online-researchers-say-2024-09-03/; Micah McCartney, "'Spamouflage': China Cyber Army Mimics Americans to Influence US Election," (September 3, 2024). *Newsweek.com*, https://www.newsweek.com/china-news-cyber-army-mimics-americans-influence-us-election-2024-1947901.
13. U.S. Department of Defense, *Summary – 2023 Cyber Strategy*, 4; Dave Aitel, et al., *China's Cyber Operations*, 8-37.
14. James A. Lewis, " How Much Have the Chinese Actually Taken?" (March 22, 2018). *CSIS.org*, https://www.csis.org/analysis/how-much-have-chinese-actually-taken.
15. James A. Lewis, "China's Economic Espionage: Why It Worked in the Past but It Won't in the Future,"(November 13, 2012). *Foreign Affairs*, https://www.foreignaffairs.com/articles/china/2012-11-13/chinas-economic-espionage.; Office of the United States Trade Representative, *Findings of the Investigation into China's Acts, Policies, and Practices related to Technological Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, (March 22, 2018). https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2018/june/section-301-investigation-fact-sheet.

NOTES

16. Federal Bureau of Investigation, *Executive Summary – China: The Risk to Corporate America*, (2019). Washington, D.C., https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf.
17. Dave Aitel, et. al., *China's Cyber Operations; Office of the United States Trade Representative, Findings of the Investigation into China's Acts, Policies, and Practices related to Technological Transfer, Intellectual Property, and Innovation Under Section 301 of the Trade Act of 1974*, (March 22, 2018). https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.
18. Nick Beecroft, "The West Should Not Be Complacent about China's Cyber Capabilities," (July 6, 2021). Washington, D.C.: Carnegie Endowment for International Peace, https://carnegieendowment.org/2021/07/06/west-should-not-be-complacent-about-china-s-cyber-capabilities-pub-84884.
19. Eric Tucker, "FBI, US Agencies Look beyond Indictments in Cybercrime Fight," (January 18, 2022). *US News and World Report*, https://www.usnews.com/news/politics/articles/2022-01-18/fbi-us-agencies-look-beyond-indictments-in-cybercrime-fight.
20. Karen A. Rasle and William R. Thompson, *The Great Powers and Global Struggle*, 1490-1990, (1994). Lexington, KY: *University of Kentucky Press*, 73-97 and 157-72; Thomas F. Lynch III, "Cyberspace: Great Power Competition in a Fragmenting Domain," (2024). Orbis 68, Issue 4, https://doi.org/10.1016/j.orbis.2024.09.007, 607-623
21. Clint Watts, "Five Generations of Online Manipulation: The Evolution of Advanced Persistent Manipulators," (March 11, 2019). *Foreign Policy Research Institute – National Security Program E-note*, https://www.fpri.org/article/2019/03/five-generations-of-online-manipulation-the-evolution-of-advanced-persistent-manipulators/. Lynch, "The Future of Great Power Competition: Trajectories, Transitions, and Prospects for Catastrophic War," 18.
22. Council on Foreign Relations, *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*, (June 2022). New York, NY: Council on Foreign Relations [CFR], Independent Task Force Report No. 80, https://www.cfr.org/task-force-report/confronting-reality-in-cyberspace; Lynch, "The Future of Great Power Competition: Trajectories, Transitions, and Prospects for Catastrophic War," 18.
23. James A. Lewis, "Sustaining Progress in International Negotiations on Cybersecurity," (July 25, 2017). The Center for Strategic and International Studies (CSIS), https://www.csis.org/analysis/sustaining-progress-international-negotiations-cybersecurity; Lynch, "The Future of Great Power Competition: Trajectories, Transitions, and Prospects for Catastrophic War," 18.
24. Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd ed.*, (2017). Cambridge: Cambridge University Press; The NATO Cooperative Cyber Defence Centre of Excellence, *The Tallinn Manual*, (last accessed September 30, 2024). Tallinn, Estonia, https://ccdcoe.org/research/tallinn-manual/.
25. In December 2023, the U.S. and ten European allies and strategic partners endorsed the Tallinn Manual as a 'Mechanism' to coordinate civilian cyber assistance to Ukraine in its struggle with Russia. The arrangement indicated the globally constrained, but sub-group viable potential for legal norms and procedures in cyber space during an era of accelerating domain fragmentation. See, U.S. Department of State, *Formalization of the Tallinn Mechanism to Coordinate Civilian Cyber Assistance to Ukraine* (December 20, 2023). Washington, D.C., https://www.state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/.
26. Mieke Eoyang and Chimene Keitner, "CyberCrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity," (February 2, 2021). *Journal of National Security, Law and Policy*, https://jnslp.com/2021/02/02/cybercrime-vs-cyberwar-paradigms-for-addressing-malicious-cyber-activity/, 327; Gary D. Brown, "Spying and Fighting in Cyberspace," (2016). *Journal of National Security Law & Policy*, https://jnslp.com/wp-content/uploads/2017/10/Spying-and-Fighting-in-Cyberspace_2.pdf.
27. Eric Tucker, "FBI, US Agencies Look beyond Indictments in Cybercrime Fight," (January 18, 2022). *APNews.com*, https://apnews.com/article/technology-indictments-crime-europe-hacking-8e97ebd22a64a28bfc4ea83c123ee1dc; University of Baltimore Law Review Staff, "Indictments Don't Deter Cyberattacks, So Why Does the U.S. Keep Using Them? An Analysis in Response to the U.S.'s Recent Indictment of Six Russian Hackers," (February 26, 2021), Baltimore, MD: *University of Baltimore Law Review*, https://ubaltlawreview.com/2021/02/26/indictments-dont-deter-cyberattacks-so-why-does-the-u-s-keep-using-them-an-analysis-in-response-to-the-u-s-s-recent-indictment-of-six-russian-hackers/.
28. Justin Sherman, "Russia's largest hacking conference reflects isolated cyber ecosystem," (January 12, 2023). *Brookings.com*, https://www.brookings.edu/articles/russias-largest-hacking-conference-reflects-isolated-cyber-ecosystem/.
29. Michael P. Fischerkeller, Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, (May 19, 2022). Oxford: Oxford University, https://academic.oup.com/book/41918.

NOTES

30. Emily O. Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn," (Winter 2022), *Cyber Defense Review* Vol. 7, No. 1, 113-120, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/CDR_V7N1_WINTER_2022_Special_Edition_r7.pdf; Jacqueline C. Schneider, "Persistent Engagement: Foundation, Evolution and Evaluation of a Strategy," (May 10, 2019); *Lawfare*, https://www.lawfaremedia.org/article/persistent-engagement-foundation-evolution-and-evaluation-strategy.
31. Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn."
32. Cyberspace Solarium Commission, *Cyberspace Solarium Commission*, (March 2020). Report, Washington, D.C.: Senator Angus King and Representative Mike Gallagher, Co-chairmen, https://cybersolarium.org/march-2020-csc-report/march-2020-csc-report/; Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn," Page?
33. Martin Libicki, *Cyberdeterrence and Cyberwar,* (2009). Santa Monica: RAND Corporation, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf,
34. Michael P. Fischerkeller and Richard J. Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," (June 23, 2017). Orbis Vol. 61, No. 3, Fall 2017, https://www.fpri.org/article/2017/06/deterrence-not-credible-strategy-cyberspace/, 381-393.
35. Richard L. Harknett and Joseph S. Nye Jr., "Is Deterrence Possible in Cyberspace?," (November 1, 2017) *International Security*, Vol. 42, No. 2, https://doi.org/10.1162/ISEC_c_00290, 199
36. Joseph Nye Jr., "Deterrence and Dissuasion in Cyberspace," (January 1, 2017). *International Security*, Vol 41, No. 3, Fall 2017, https://doi.org/10.1162/ISEC_a_00266, 44-71; Harknett and Nye, "Is Deterrence Possible in Cyberspace?," 199.
37. Jacquelyn C. Schneider, Emily O. Goldman, and Michael Warner, eds., *Ten Years In: Implementing Strategic Approaches to Cyberspace*, (2020). Newport, RI: U.S. Naval War College – Newport Papers #45, https://digital-commons.usnwc.edu/usnwc-newport-papers/45/.
38. Emily O. Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn."
39. Chris Inglis, "Cybersecurity Cooperation," (May 11, 2022), Remarks at The Lowy Institute, Sydney Australia. Locationhttps://www.lowyinstitute.org/publications/regional-cybersecurity-cooperation-evolving-geopolitical-landscape.
40. Schneider, Goldman, and Warner, eds., *Ten Years In: Implementing Strategic Approaches to Cyberspace*, 40-41; Max Smeets and Herb Lin, "An Outcome-Based Analysis of US Cyber Strategy of Persistence and Defend Forward," (November 28, 2018). *Lawfare*, https://www.lawfareblog.com/outcome-based-analysis-us-cyber-strategy-persistence-defend-forward; Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn."
41. James A. Lewis, "Private Actors Roles in International Cybersecurity Agreements – Unlearned Lessons," (Winter 2022). *The Cyber Defense Review* ,Vol. 6, No. 1, https://cyberdefensereview.army.mil/Portals/6/Documents/2022_winter/04_Lewis_CDR_V7N1_WINTER_2022.pdf?ver=l865DxcB5fL5jJxwk7n9eg%3d%3d, 34-39.
42. Fischerkellers, Goldman, and Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, page?
43. Thomas L. Lynch III, "Cyberspace: Great Power Competition in a Fragmenting Domain," (September 2024). *Orbis* Volume 68, Issue 4, https://www.sciencedirect.com/science/article/abs/pii/S0030438724000516, 620-621.
44. Paul Nakasone, "A Cyber Force for Persistent Operations," (2019). *Joint Forces Quarterly* Vol. 92, No. 1, 10-14, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf; Smeets and Lin, "An Outcome-Based Analysis of US Cyber Strategy of Persistence and Defend Forward.";" Lynch, "Cyberspace: Great Power Competition in a Fragmenting Domain," 621.
45. Paul Nakasone, "A Cyber Force for Persistent Operations;" Paul Nakasone, "Posture Statement of General Paul M. Nakasone, Commander, U.S. Cyber Command before the 117th Congress," (April 5, 2022). https://www.cybercom.mil/Media/News/Article/2989087/posture-statement-of-gen-paul-m-nakasone-commander-us-cyber-command-before-the/. Lynch, "Cyberspace: Great Power Competition in a Fragmenting Domain," 621.
46. U.S. Department of Defense, *Fact Sheet: 2022 National Defense Strategy,* (March 2022). https://media.defense.gov/2022/Mar/28/2002964702/-1/-1/1/NDS-FACT-SHEET.PDF, 2.
47. Michael P. Fischerkeller, "What Does the 2022 NDS Fact Sheet Imply for the Forthcoming Cyber Strategy?", (May 3, 2022). *Lawfare,* https://www.lawfareblog.com/what-does-2022-nds-fact-sheet-imply-forthcoming-cyber-strategy.
48. *Cyberspace Solarium Commission (CSC) Report*, 1-7.
49. *Cyberspace Solarium Commission (CSC) Report*, 26-30.
50. U.S. Department of Defense, *Fact Sheet: 2022 National Defense Strategy,* 2.

NOTES

51. Emily O. Goldman, "From Reaction to Action: Adopting a Competitive Posture in Cyber Diplomacy," (Fall 2020). *Texas National Security Review* Vol. 3, No. 4, https://tnsr.org/2020/09/from-reaction-to-action-adopting-a-competitive-posture-in-cyber-diplomacy/; Sue Gordon and Eric Rosenbach, "America's Cyber-Reckoning: How to Fix a Failing Strategy," (January/February 2022). *Foreign Affairs* Vol. 101, No. 1: 10-21, https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning; Max Sweets, "The Strategic Promise of Offensive Cyber Operations," (Fall 2018). *Strategic Studies Quarterly,* Vol. 12, No. 3: 105, https://www.airuniversity.af.edu/; *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*, (June 2022). New York, NY: Council on Foreign Relations [CFR], Independent Task Force Report No. 80.
52. Florian J. Egloff and James Shires, "The Better Angels of Our Digital Nature? Offensive Cyber Capabilities and State Violence," (October 12, 2021). *European Journal of International Security*, 1-20, https://www.cambridge.org/core/journals/european-journal-of-international-security/article/better-angels-of-our-digital-nature-offensive-cyber-capabilities-and-state-violence/B225F961FD2212E34FDB0B267A1CB5E6
53. Goldman, "Paradigm Change Requires Persistence – A Difficult Lesson to Learn."
54. Erica D. Lonergan and Shawn W. Lonergan, *Escalation Dynamics in Cyberspace*, (2023). Oxford: Oxford University Press, 2023), Chapters 1 and 6; J.E. Barnes and Thomas Gibbons-Neff, "U.S. Carried Out Cyber Attacks on Iran," (June 22, 2019). *New York Times*, https://www.nytimes.com/2019/06/22/us/politics/us-iran-cyber-attacks.html; R. Chesney, "The Legal Context for CYBERCOM's Reported Operations Against Iran," June 24, 2019. *Lawfare.com*, https://www.lawfareblog.com/legal-context-cybercoms-reported-operations-against-iran; Erica D. Bohrghard, "What a US Operation Against Russian Trolls Predicts About Escalation in Cyberspace," (March 22, 2019). *War on the Rocks*, https://warontherocks.com/2019/03/what-a-u-s-operation-against-russian-trolls-predicts-about-escalation-in-cyberspace/.
55. Michael Warner, "A Brief History of Cyber Conflict," (2020). In *Ten Years In: Implementing Strategic Approaches to Cyberspace*, edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner. Newport, RI: U.S. Naval War College – Newport papers #45, 2020, 20.
56. Chris Demchak, "When Irregular Becomes Everywhere: The Cybered Fight in Unwanted Places," (July 13, 2022). *Modern War Institute*, https://mwi.usma.edu/when-irregular-becomes-everywhere-the-cybered-fight-in-unwanted-places/
57. The Cyber National Mission Force, *Before the Invasion: Hunt Forward Operations in Ukraine*, (November 28, 2022). Washington, D.C: USCYBERCOM, https://nsarchive.gwu.edu/sites/default/files/documents/rmsj3h-751x3/2022-11-28-CNMF-Before-the-Invasion-Hunt-Forward-Operations-in-Ukraine.pdf; Anastasia Obis, "Cyber Command Finishes its First 'Hunt Forward' Operation in Latin America," (June 30, 2023). *GovCIO.com*, https://governmentciomedia.com/cyber-command-finishes-its-first-hunt-forward-operation-latin-america.
58. U.S. Department of Defense, *Summary – 2023 Cyber Strategy of the Department of Defense*, 6-7; David E. Sanger and Mark Mazzetti, "US had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict," (February 16, 2016). *The New York Times*, https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html; Idrees Ali and Phil Stewart, "Exclusive: U.S. Carried out Secret Cyber Strike on Iran in Wake of Saudi Oil Attack: Officials," (October 16, 2019). *Reuters*, https://www.reuters.com/article/us-usa-iran-military-cyber-exclusive/exclusive-u-s-carried-out-secret-cyber-strike-on-iran-in-wake-of-saudi-oil-attack-officials-idUSKBN1WV0EK; Michael Martelle, ed., *USCYBERCOM After Action Assessments of Operation GLOWING SYMPHONY*, (January 21, 2020). Washington, DC: GWU National Security Archive, https://nsarchive.gwu.edu/briefing-book/cyber-vault/2020-01-21/uscybercom-after-action-assessments-operation-glowing-symphony; Florian J. Egloff, "Public Attribution of Cyber Intrusions," (Winer 2020). *Journal of Cybersecurity* Vol. 6, No. 1, https://doi.org/10.1093/cybsec/tyaa012, 1-12; Florian J. Egloff and Max Smeets, "Publicly Attributing Cyber Attacks: A Framework," (March 10, 2021). *Journal of Strategic Studies*, Vol 36, No 3, 1–32. https://doi.org/10.1080/01402390.2021.1895117.
59. Paul Nakasone, "A Cyber Force for Persistent Operations;" Paul Nakasone and Michael Sulmeyer, "How to Compete in Cyberspace," (August 25, 2020). *Foreign Affairs*, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.
60. U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority, A Command Visions for US Cyber Command*, (April 2018). Washington, D.C.; https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf, 1-3.

NOTES

61. Fischerkeller and Harknett, "Deterrence is Not a Credible Strategy for Cyberspace," 381-393.
62. Robert Chesney, "The Law of Military Cyber Operations and the New NDAA," (July 26, 2018). *Lawfare*, https://www.lawfaremedia.org/article/law-military-cyber-operations-and-new-ndaa.
63. Fischerkeller, "What Does the 2022 NDS Fact Sheet Imply for the Forthcoming Cyber Strategy?"
64. Sean Lyngaas, "U.S. Military Links Prolific Hacking Group to Iranian Intelligence." (January 12, 2022). *CNN.com*, https://edition.cnn.com/2022/01/12/politics/iran-cyber-command-hacking-muddywater/index.html.
65. Robert Chesney and Max Smeet, "Intervention: Exploring Cyber Conflict and Competition," (October 20, 2020). *War on the Rocks*, https://warontherocks.com/2020/10/the-dynamics-of-cyber-conflict-and-competition/
66. Jim Garamone, "Cyber Command, NSA Successes Point Way to Future," (March 8, 2023). *Defense.gov*, https://www.defense.gov/News/News-Stories/Article/Article/3322765/cyber-command-nsa-successes-point-way-to-future/; National Security Agency, "How NSA, U.S. Cyber Command are defending midterm elections: One team, one fight," (August 25, 2022). NSA.gov, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3136987/how-nsa-us-cyber-command-are-defending-midterm-elections-one-team-one-fight/.
67. Lizbeth Perez, "CYBERCOM Working 25 'Hunt-Forward' Missions This Year," (September 5, 2024). *MeriTalk.com*, https://cdn.meritalk.com/articles/cybercom-working-25-hunt-forward-missions-this-year/; Chauncey Goss, "DoD's FY24 Cyber Budget," (April 17, 2023). *Federal Budget IQ.com* https://federalbudgetiq.com/insights/dods-fy24-cyber-budget/
68. Chris Demchak, "Five Reasons Not to Split Cyber Command from the NSA Any Time Soon – If Ever," (March 5, 2021). *War on the Rocks,* https://warontherocks.com/2021/03/five-reasons-not-to-split-cyber-command-from-the-nsa-any-time-soon-if-ever/.
69. Paul Nakasone, "Posture Statement of General Paul M. Nakasone, Commander, US Cyber Command before the 117th Congress."
70. Ellen Nakashima and Tim Starks, "NSA, Cyber Command should continue to share a leader, a key review suggests," (December 22, 2022). *The Washington Post*, https://www.washingtonpost.com/politics/2022/12/22/nsa-cyber-command-should-continue-share-leader-key-review-suggests/.
71. Nakashima and Starks, "NSA, Cyber Command should continue to share a leader, a key review suggests."
72. Anna Scherbina, "How much do US businesses lose due to malicious cyber activity?" (May 3, 2024). *The Hill.com*, https://thehill.com/opinion/cybersecurity/4641199-cyberattack-businesses-money-loss-malicious-cybersecurity/; Anna Ribeiro, "FBI warns of increased cyber threats to expanding US renewable energy sector," (July 2, 2024). *IndustrialCyber.com*, https://industrialcyber.co/threats-attacks/fbi-warns-of-increased-cyber-threats-to-expanding-us-renewable-energy-sector/; Michael J. Mazarr, Tim Sweijs and Daniel Tapia, *The Sources of Renewed National Dynamism – RAND Report -RRA2611-3*, (April 30, 2024). https://www.rand.org/pubs/research_reports/RRA2611-3.html.
73. U.S. Cyber Command, *Achieve and Maintain Cyberspace Superiority, A Command Visions for US Cyber Command*, 4-5.
74. Jaclyn Kerr and Alexander Campbell, *Workshop Summary: Strategic Competition in Cyberspace: Challenges and Implications*, (July 10, 2019). Livermore, California: Center for Global Strategic Research, Lawrence Livermore National Laboratory, https://cisac.fsi.stanford.edu/publication/strategic-competition-cyberspace-challenges-and-implications.
75. Demchak, "Five Reasons Not to Split Cyber Command from the NSA Any Time Soon – If Ever."
76. Congressional Research Service, *FY2023 NDAA: Cyber Personnel Policies*, (March 6, 2023). Washington, D.C.: CRS Report R47270, https://crsreports.congress.gov/product/pdf/R/R47270, 1-3; Mark Pomerleau, "US Cyber Command releases first full budget," (March 13, 2023). *Defense Scoop*, https://defensescoop.com/2023/03/13/us-cyber-command-releases-first-full-budget/.
77. Pomerleau, "US Cyber Command releases first full budget."
78. Alan Suderman, "Global War on Ransomware? Hurdles Hinder the US Response," (June 5, 2021). *Associated Press*, https://apnews.com/article/europe-hacking-health-coronavirus-pandemic-technology-5d69e46750abd3b40fc9adf395869c7d.; Erica Lonergan and Mark Montgomery, "What Is the Future of Cyber Deterrence?" (2021). *SAIS Review of International Affairs* Vol. 41, No. 2, 61-73, https://muse.jhu.edu/article/852327.
79. *Cyberspace Solarium Commission (CSC) Report*, 28-29.
80. The White House, *National Cybersecurity Strategy*, (March 2023). https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, 14-15.

NOTES

81. As of mid-2024, the U.S. Government is advancing slowly toward more robust, interagency-wide, coordinated cyber

operations. The USCYBERCOM-NSA Integrated Joint Cyber Center, launched in 2018, is a productive node for agency-wide collaboration on cyber defense. Non-DOD, government agency cyber persistence and hunt forward operations are inching forward. The Cybersecurity and Infrastructure Security Agency (CISA) established and exercised Red Team "hunt" operations in support of national defense in depth during 2023 and 2024, but its capabilities are nascent. The FBI has special Cyber Action Team (CAT) of approximately 65 members to deploy across the globe in response to malicious cyber activity threatening U.S. public safety, national security or economic security. This is an incident reaction team not yet a hunt forward one. See, Mark Pomerleau, "Five years in, a look at how Cybercom and NSA's Integrated Cyber Center improved coordination of operations," (May 31, 2023). *DefenseScoop.com*, https://defensescoop.com/2023/05/31/five-years-in-a-look-at-how-cybercom-and-nsas-integrated-cyber-center-improved-coordination-of-operations/; Cybersecurity and Infrastructure Securaity Agency, "CISA Red Team's Operations Against a Federal Civilian Executive Branch Organization Highlights the Necessity of Defense-in-Depth," (July 11, 2024). CISA.gov, Cybersecurity Advisory, Alert Code: AA24-193A, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-193a; Federal Bureau of Investigation, "Meet the Cyber Action Team," (July 23, 2024). *FBI.com*, https://www.fbi.gov/news/stories/meet-the-cyber-action-team.

THE CYBER DEFENSE REVIEW

CONTINUE THE CONVERSATION ONLINE

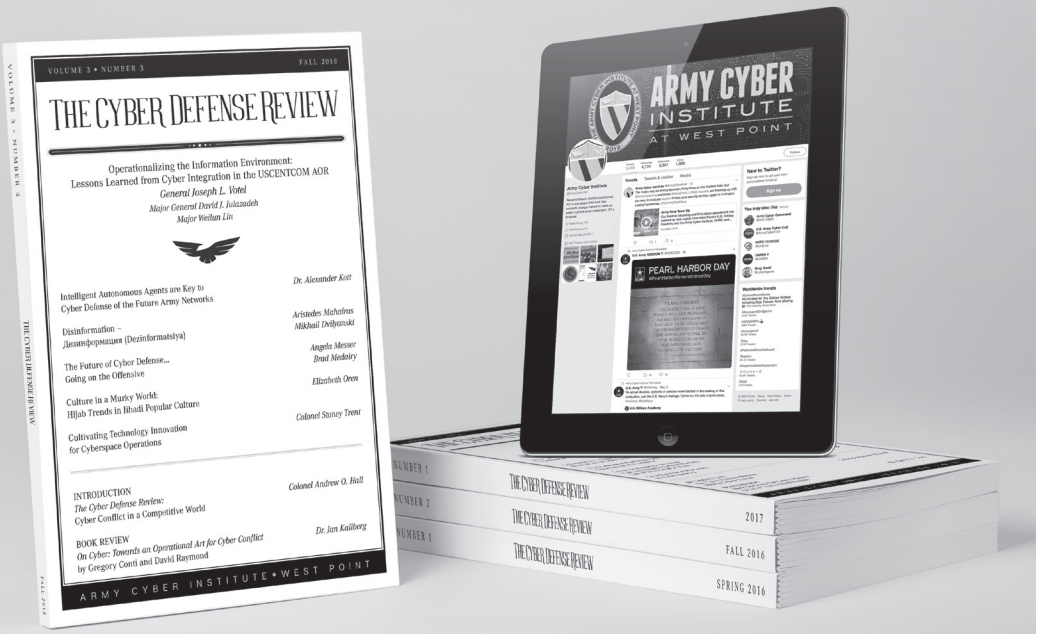
CyberDefenseReview.Army.mil

AND THROUGH SOCIAL MEDIA

Facebook @ArmyCyberInstitute

LinkedIn @LinkedInGroup

Twitter @ArmyCyberInst
@CyberDefReview



ARMY CYBER INSTITUTE ◆ WEST POINT PRESS

WEST POINT
PRESS

THE CYBER DEFENSE REVIEW IS A NATIONAL RESOURCE THAT CONTRIBUTES TO THE CYBER DOMAIN, ADVANCES THE BODY OF KNOWLEDGE, AND CAPTURES A UNIQUE SPACE THAT COMBINES MILITARY THOUGHT AND PERSPECTIVE FROM OTHER DISCIPLINES.