ACCELERATE CHANGE
OR LOSE THE INFORMATION WAR

Karen Guttieri

The United States Air Force must accelerate change or lose an information-cyber war that is already hot and holds at risk American social, economic, and political cohesion. The Air Force has launched promising organizational and technological initiatives including an "integration imperative" recognizing the interdisciplinary, techno-sociological character of information warfare. At the same time, the Air Force has removed cyber from its mission statement. Moreover, force development does not progress past digital literacy, cyber hygiene, and information technology training. To win, the Air Force must develop and promote strategists to overcome vulnerabilities and seize opportunities in the cyberspace domain and information environment.

In August 2020, General CQ Brown Jr., chief of staff of the United States Air Force, warned of "rapid technology development and diffusion" driving change in the strategic environment.[1] American innovations of the late twentieth century had delivered instant global connectivity, operational technology, geographic positioning, and other capabilities that changed daily life and shaped relative military power and power projection.[2] Twenty years later, American economic, social, and warfighting advantages from these advances are eroding. The Air Force's high-tech, robustly networked systems and the highly networked public they protect have become large attack surfaces. In response, Brown ordered, "accelerate change or lose."

In October 2020, a Joint Force wargame showed how loss might play out. By admission of the Vice Chairman of the Joint Chiefs of Staff General John E. Hyten, the US Joint warfighting concept "failed miserably" when the red team denied US forces *in the information environment*, impairing communications and command and control, and rendering useless many key capabilities.[3] The wargame invalidated twenty-

1. Charles Q. Brown Jr., *Accelerate Change Or Lose* (Washington, DC: Headquarters, Department of the Air Force, August, 2020), 1. The author would like to thank Kevin L. Parker and Contessa Hannig for their essential advice and insight during the drafting of this article.

2. Brown, *Accelerate Change*, 4.

3. Emphasis added. John E. Hyten remarks on defense technology at the Emerging Technologies Institute, July 26, 2021, Video, 12:21, https://www.c-span.org/; and Chris Dougherty "Confronting Chaos: A New Concept for Information Advantage," War on the Rocks, September 9, 2021, https://warontherocks.com/.

year-old assumptions. The United States could no longer take information superiority for granted.

Information warfare—a concept that involves both technical and human elements—is already a hot war. China spies, steals blueprints of American warplanes, and purloins massive amounts of personal data. Russia reaches through cyberspace to attempt to disrupt American elections and deliver propaganda that further divides everyday Americans. "Our adversaries have brought strategic competition to the nation's front door," writes Sixteenth Air Force Commander General Timothy Haugh, "by engaging the United States' population in the information environment."[4] With this in mind, what are the prospects for the Air Force to "accelerate change or lose" the information war?

Historically, multiple forces drive military change. Civilian intervention, an external force, is one, but this article will instead focus on two drivers the Air Force controls—strategic assessment and officer development.[5] Assessment that leads to reconsideration of a strategic goal or the concept of operations in relation to that goal is an impetus to change.[6] This is happening today. Militaries also change through officer development and promotion. This element of Brown's action order "A"—develop Airmen—needs attention.

The Information War

> *"Plus, China and Russia are trying to take out our internet every day. People really like the internet. They're always checking it."*
>
> - Steve Carell as General Mark R. Naird

The fictional commander of Space Force, General Mark Naird, in the television comedy of the same name, complained to his therapy group of constant attacks.[7] In 2019, the real-life Air Force lieutenant general responsible for Air Force cyber and intelligence declared, "Right now, today, in the cyber domain, in information operations, I am not at peace. I am in persistent conflict."[8] A Russian diplomat later echoed her comment, saying, "The war [in cyberspace] is underway and unfolding very intensively. No matter how hard we may try to say that all this is disguised and that it

4. Timothy D. Haugh, Nicholas J. Hall, and Eugene H. Fan, "16th Air Force and Convergence for the Information War," *Cyber Defense Review* (Summer 2020): 30.

5. Deborah D. Avant, *Political Institutions and Military Change: Lessons from Peripheral Wars* (Ithaca, NY: Cornell University Press, 1994); and Stephen Peter Rosen, *Winning the Next War* (Ithaca NY: Cornell University Press, 1991).

6. Rosen, *Next War*, 7.

7. Eriq Gardner, "Trump's Space Force Already Lost Its First Battle," *Hollywood Reporter*, June 5, 2020, https://www.hollywoodreporter.com.

8. VeraLinn Jamieson, quoted in Shaun Waterman, "Cyber Flight Plan Outlines USAF Efforts to Take on Hybrid Warfare," *Air Force Magazine*, September 19, 2019, https://www.airforcemag.com/.

isn't that war or this war, in actual fact, military activities in cyberspace are in full swing."[9] Dynamic cyberattack maps illustrate the complexity of the battlespace.[10]

Scholars debate what this all means. Some see it as hyperbole because the confrontation is mostly waged as espionage, subversion, and sabotage.[11] Others argue nonkinetic cyber operations merely support kinetic operations.[12] Those critics miss the point that the nonkinetic fight is reshaping any future kinetic battlefield, and perhaps overshadowing the relevance of the kinetic battlefield.

Information warfare is "the employment of military capabilities in and through the information environment to deliberately affect adversary human and system behavior and to preserve friendly freedom of action during cooperation, competition, and conflict."[13] This not-yet-doctrinal description is consistent with the mid-twentieth-century cybernetics field's interest in control of industrial production and thought processes and its depiction of community as a function of information transmission.[14] It aligns with Russian and Chinese constructs of information warfare as involving technical *and social* components.

Information warfare was first introduced by American scientist Thomas P. Rona in a 1976 study anticipating advances in human use of the electromagnetic spectrum.[15] Rona explained an aerial attack as an information system, reliant on electronics, computation, and communications, with complex internal and external information flows. Pilots using fly-by-wire do not directly maneuver their aircraft with mechanical links. Instead, a computer reads the pilot's input to determine what signals to send the control actuators for yaw, pitch, and roll.[16] Systems are vulnerable at the seams of external information flow.

Discussion of information warfare intensified in the 1990s after US success in the Gulf War. Advanced command, control, communications, intelligence, surveillance, and reconnaissance capabilities, instantaneous communications, global positioning technologies, and precision strike capabilities gave the US game-changing advantages.

---

9. "Full-Blown Warfare in Cyberspace in Progress, Says Russian Diplomat," Tass News Agency, December 16, 2021, https://tass.com/world/1376491.

10. Fireeye "Cyber Threat Map," accessed January 12, 2022, https://www.fireeye.com/; and National Security Archive, "CyberWar Map," accessed January 12, 2022, https://embed.kumu.io/.

11. Thomas Rid, *Cyber War Will Not Take Place* (Oxford: Oxford University Press, 2018).

12. Martin C. Libicki, *Cyberspace in Peace and War* (Annapolis, MD: Naval Institute Press, 2016), 161.

13. George M. Reynolds, "Achieving Convergence in the Information Environment," *Air & Space Power Journal* 34, no. 4 (Winter 2020): 6; and Sandeep Mulgund, "Memorandum for: C2 of Operations in the Information Environment (OIE) Working Group" (Washington, DC: Department of the Air Force, A3, September 15, 2020).

14. Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine,* Reissue of the 1961 2nd ed. (Cambridge, MA: MIT Press, 2019); and Alexander Klimburg, *The Darkening Web* (London: Penguin, 2017), 23–25, 219.

15. Thomas P. Rona, *Weapon Systems and Information War* (Seattle, WA: Boeing Aerospace Company, 1976).

16. Ilie Nicolin and Bogdan Adrian Nicolin, "The Fly-by-Wire System," *INCAS Bulletin* 11, no. 4 (December 2019), https://www.researchgate.net/.

The United States Air Force owned the skies. The then-Soviet Russians called this a military-technical revolution; Americans called it a revolution in military affairs.

The Department of Defense fostered the internet, but the private sector soon became the locus of information technology innovation.[17] In fact, the Air Force now looks to the private sector for "IT as a Service," to free military cyber experts from information technology duties in order to focus on the more critical offensive and defensive cyber operations.[18] Amazon Web Services partners with the Air Force to test cloud capabilities at the tactical edge.[19] Military acquisition and logistics personnel and defense innovation units navigate a complex innovation ecosystem, leveraging and relying on private-sector advances.

In about 2013, America's competitors began to catch up. General Paul M. Nakasone, commander of US Cyber Command and director of the National Security Agency, referred to "a strategic inflection point" in which adversaries began operating "continuously against critical infrastructure, government networks, defense industries, and academia—both in America and abroad."[20] Technology dependence created increasingly complex vulnerabilities, many in the civilian sector outside the control of the military.

Today, information vulnerabilities extend to space. Satellites, their ground stations, and data links are essential to communications, computing and network systems, geographic positioning, weather prediction, satellite TV and radio, phones, broadband, air traffic control, even telling the time.[21] Russia and China threaten with antisatellite weapons, but the Department of Defense Space Development Agency director worries more about cyber and supply-chain exploitations. "It doesn't matter if I have one satellite or if I have 1,000 satellites, those type of attacks may have the ability to take them all out."[22]

And people really like the internet. On December 7, 2021, Amazon Web Services—controlling 33 percent of the global cloud infrastructure—suffered an outage. Parts of Amazon's enormous retail operations ground to a halt; iRobot Roomba vacuums resisted orders; and websites dropped offline, including learning management programs,

17. Karen Guttieri, "Governance, Innovation, and Information and Communications Technology for Civil-Military Interactions," *Stability* 3, no. 1 (2014): 6. doi:10.5334/.

18. K. Houston Waters, "Air Force Deploys Commercial IT Capability," Air Force Public Affairs, October 7, 2020, https://www.af.mil/.

19. Amazon Web Services (AWS) Public Sector Blog Team, "Bringing Cloud Capability to the Air Force at the 'Speed of Mission Need,'" AWS Public Sector Blog, May 7, 2021, https://aws.amazon.com/.

20. Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2019): 11, https://ndupress.ndu.edu/.

21. Meg King and Sophie Goguichvili, "Cybersecurity Threats in Space: A Roadmap for Future Policy," Ctrl Forward (blog) Science and Technology Innovation Program, Wilson Center, October 8, 2020, https://www.wilsoncenter.org/.

22. Sandra Irwin, "DoD Space Agency: Cyber Attacks, Not Missiles, Are the Most Worrisome Threat to Satellites," *Space News*, April 14, 2021, https://spacenews.com/.

causing universities to cancel exams during finals week.[23] While the incident is a cautionary tale for the Air Force as it shifts its basic computing services to this commercial sector, it could be much worse.

Cyberattacks can seize control of an operating system to produce physical effects. In 2010, the Stuxnet worm, the first known virus to cripple hardware, caused some of Iran's nuclear reactors to self-destruct. In February 2021, a hacker using remote-access software broke into the control system of a municipal water treatment facility and attempted to increase lye in the water to harmful levels.[24]

The US Cybersecurity Infrastructure Security Agency identifies sixteen sectors as critical infrastructure meaning "incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety."[25] Some say cyber weapons are strategic because an attack on critical infrastructure could harm large civilian populations.[26] Indeed, this issue is discussed widely in United Nations and other international fora.

Still, cyber weapons do have their limitations. Zero-day opportunities are time limited because once known they can be patched. The intruder must manage a trade-off between maintaining an opportunity for espionage and the execution of malware that could divulge their presence in the system. An effective hacker must be aware of the complex physical and social systems of the target.[27]

And malware once released can boomerang. The National Security Agency developed cyber tools that were stolen by the Shadow Brokers group and released beginning August 2016.[28] Purportedly among these was EternalBlue, a penetration tool. In 2017, North Korean hackers used EternalBlue in the WannaCry ransomware attack that affected computers in more than 150 countries and crippled the United Kingdom's National Health Service for days.[29] Then Russian military hackers used it in the

23. Annie Palmer, "Dead Roombas, Stranded Packages and Delayed Exams: How the AWS Outage Wreaked Havoc across the US," CNBC (online), December 9, 2021, https://www.cnbc.com/.

24. Andy Greenberg, "A Hacker Tried to Poison a Florida City's Water Supply, Officials Say," *Wired*, February 8, 2021, https://www.wired.com/.

25. "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency (website), n. d., accessed January 13, 2022, https://www.cisa.gov/critical-infrastructure-sectors.

26. Sarah Kreps and Jacquelyn Schneider, "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond Effects-Based Logics," *Journal of Cybersecurity* 5, no. 1 (2019), https://academic.oup.com/.

27. "Critical Infrastructure Sectors," Cybersecurity and Infrastructure Security Agency (website), n. d., accessed January 13, 2022, https://www.cisa.gov/; and M. A. Thomas, "Unleashing the US Military's Thinking about Cyber Power," War on the Rocks, November 4, 2021.

28. Scott Shane, Nicole Perlroth, and David E. Sanger, "Security Breach and Spilled Secrets Have Shaken the NSA to Its Core," *New York Times*, November 12, 2017, https://www.nytimes.com/; and Lily Hay Newman, "The Leaked NSA Spy Tool that Hacked the World," *Wired,* March 7, 2018, https://www.wired.com/.

29. Roger Collier, "NHS Ransomware Attack Spreads Worldwide," *Canadian Medical Association Journal*, 189, no. 22 (June 2017): E786–87, https://doi.org/.

NotPetya attack that caused billions in damage worldwide.[30] Initially targeting Ukraine, NotPetya spread rapidly, affecting systems around the world, including Rosneft, Russia's state oil company.[31]

Like the IT serving them, social systems are wired for connectivity. Social media interaction and outsourcing cognition have made US military personnel, other national security practitioners, and everyday Americans prime targets for online psychological manipulation.[32] And online behavior has proven successful at shaping behavior in real life. In 2016 Russians, seeking to widen partisan US divisions, used fake Facebook accounts and armies of bots and trolls to attract Americans to at least eight political campaign rallies, including competing events on the same day in New York City.[33]

The internet empowers social mobilization at speed and scale with global reach at low cost.[34] Weapons like those employed by Russia enable states to attack below the threshold of armed conflict in the so-called gray zone. Anonymity offers weaker actors an opportunity to inflict pain without consequences. Attribution is difficult and doing so reveals one's own abilities. For these reasons, many believe cyberspace operations favor the offense.[35] Indeed, current US policy might be characterized as the best defense is a good offense.

The US strategy is "persistent engagement" through cyberspace. "We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."[36] This requires continuous access, but an intrusion intended to defend can also provide cover for an attack. In 2007, Israeli planes hacked Syrian air defenses on the ground so the Syrians would not detect incoming Israeli strikes against a suspected nuclear reactor complex.[37] In other words, one

30. US Department of Justice (USDOJ) Office of Public Affairs, "North Korean Regime-Backed Programmer Charged with Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," USDOJ (website) September 6, 2018, https://www.justice.gov/; and USDOJ Office of Public Affairs, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive actions in Cyberspace," USDOJ (website) October 19, 2020, https://www.justice.gov/.

31. Andy Greenberg, "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/.

32. Rosanna. E. Guadagno and Karen Guttieri, "Fake News and Information Warfare," in *Research Anthology on Fake News, Political Warfare, and Combatting the Spread of Misinformation*, ed. Mehdi Khosrow-Pour (Hershey, PA: IGI Global, 2020).

33. Alicia Parlapiano and Jasmine C. Lee, "The Propaganda Tools Used by Russians to Influence the 2016 Election," *New York Times*, February 16, 2018, https://www.nytimes.com/.

34. Kevin L. Parker, "The Utility of Cyberpower," *Military Review* 94, no. 3 (2014); and Audrey Kurth Cronin, "Cyber-Mobilization: The New Levée En Masse," *Parameters* 36, no. 2 (2006), https://press.armywarcollege.edu/.

35. Joseph S. Nye Jr., "Cyber Power," paper (Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2020), 5, https://www.belfercenter.org/; and William J. Lynn III, "Defending a New Domain," *Foreign Affairs* (September/October 2010), https://www.foreignaffairs.com/.

36. US Department of Defense (DOD), *Summary: Department of Defense Cyber Strategy 2018* (Washington, DC: DOD, 2018), https://media.defense.gov/.

37. Kim Zetter, "Hacker Lexicon: What Are CNE and CNA?" *Wired*, July 6, 2016, https://www.wired.com/.

cannot assume an electronic attack will be confined to a single purpose. The resulting risk of unintended escalation amounts to a cybersecurity dilemma.[38]

Strategic Competitors in the Information Environment

The 2018 *United States National Cyber Strategy* declared, "persistent engagement in cyberspace is already altering the strategic balance of power."[39] The US Intelligence Community in its *2021 Annual Threat Assessment* reports greatest concern about China, Russia, Iran and North Korea.[40] These adversaries seek access to critical infrastructure and to undermine, through digital influence campaigns, the American public's confidence in institutions and the confidence of Allies and partners in American foreign policy commitments. Airmen and Guardians must understand the mindsets of America's most powerful competitors in cyberspace, China and Russia.

China

The Intelligence Community describes China's agenda as "the expansion of technology-driven authoritarianism around the world."[41] The People's Republic of China is the global leader in surveillance and censorship technology. The government worries information technology might aid social mobilization and seeks internal sovereign control. China launched an internet-based censorship and surveillance program called the "Golden Shield Project" in 2003, also known as the "Great Firewall of China."[42]

The People's Republic of China has forced concessions from American corporations including Apple, Disney, Facebook, Google, and Microsoft. Apple, for example, portrayed disputed islands on its maps as larger than they are, and Facebook ran Chinese government advertisements denying persecution of Uyghur Muslims.[43] The Chinese Central Propaganda Department's media censorship extends to Hollywood.[44] China thus exerts an authoritarian variant of soft power.

---

38. Ben Buchanan, *The Cybersecurity Dilemma : Hacking, Trust and Fear between Nations* (Oxford: Oxford University Press, 2017).

39. Donald J. Trump, *National Cyber Strategy of the United States of America* (Washington DC: The White House, September 2018), https://trumpwhitehouse.archives.gov/.

40. Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the US Intelligence Community* (Washington, DC: ODNI, April 9, 2021), 8, 10–11, 14, 15–16, https://www.dni.gov/.

41. ODNI, *Annual Threat Assessment.*

42. The International Institute for Strategic Studies (IISS), "Cyber Capabilities and National Power: A Net Assessment," research paper, IISS (blog), June 28, 2021, 89, https://www.iiss.org/.

43. Katie Canales, "How Silicon Valley Came to Depend on China for Success–and Why It's Bent Over Backward to Stay in the Government's Good Graces," *Business Insider*, December 15, 2021, https://www.businessinsider.com/.

44. James Tager, *Made in Hollywood, Censored by Beijing* (New York: PEN America, September 2020), https://pen.org/.

The Chinese domestic development strategy includes a "military-civil fusion" of science and technology industries.[45] Huawei, founded in 1987 by a former engineer in China's People's Liberation Army, is currently the world's largest telecommunications equipment manufacturer.[46] Many countries, including the United States, Australia, Japan, and some European states, ban Chinese technology firms from their 5G infrastructure over security concerns. China is developing other markets.

The Digital Silk Road initiative, part of China's global Belt and Road Initiative since 2015, builds information networks and infrastructure to position China to set technology standards and to extend the reach of its surveillance and content control.[47] Each month a billion people spend time on the Chinese video app TikTok that rivals Silicon Valley's most notorious persuasive technology for its addictiveness and ability to read the minds of its users.[48] Its algorithm keeps users engaged while the app siphons, at user consent, massive amounts of personal data.

China reorganized stovepiped agencies into the Chinese Strategic Support Forces in 2015 to bring together cyber espionage and psychological warfare.[49] Chinese espionage imperils US industry and national security. Hackers linked to the People's Liberation Army are believed to have stolen information about the F-35 stealth fighter, the Air Force's F-22 platform, and numerous other weapon systems from the B-2 stealth bomber to space-based lasers.[50]

In 2020, the US Attorney General indicted four Chinese military hackers, linking large-scale data thefts from the US Office of Personnel Management, Marriott hotels, Anthem insurance, and Equifax to the Chinese government.[51] These are not one-off heists; they are part of an integrated campaign. Chinese intelligence services have used this combination of travel, health, credit, and other information to identify US intelligence officers, and to identify and target recruits.[52]

---

45. Office of the Secretary of Defense (OSD), *Military and Security Developments Involving the People's Republic of China 2021: Report to Congress* (Washington, DC: OSD, November 3, 2021), IV, https://media.defense.gov/.

46. Stephen P. Mulligan and Chris D. Linebaugh, *Huawei and US Law,* R46693 (Washington, DC: Congressional Research Service, February 21, 2021), summary, https://crsreports.congress.gov/.

47. Joshua Kurlantzick, "Assessing China's Digital Silk Road Initiative: A Transformative Approach to Technology Financing or a Danger to Freedoms," interactive article, Council on Foreign Relations, December 18, 2020, https://www.cfr.org/.

48. Ben Smith, "How TikTok Reads Your Mind," *New York Times*, December 5, 2021, https://www.nytimes.com/.

49. IISS, "Net Assessment," 91–92.

50. Eli Fuhrman, "How China Stole the Designs for the F-35 Stealth Fighter," 1945, July 15, 2021, https://www.19fortyfive.com/.

51. Garrett M. Graff, "China's Hacking Spree Will Have a Decades-Long Fallout," *Wired*, February 11, 2020, https://www.wired.com/.

52. Richard J. Harknett and Max Smeets, "Cyber Campaigns and Strategic Outcomes," *Journal of Strategic Studies* (published online March 2020), https://doi.org/.

Russia

The Intelligence Community considers Russia a top cyber threat with demonstrated capabilities including cyber espionage, influence operations, and attack (the ability to damage infrastructure such as underwater cables and industrial control systems during a crisis). Russia added "information-operations troops" to the armed forces in 2017 to conduct both cyber and information operations, including traditional psychological operations.[53] Russian President Vladmir Putin is said to personally control a centralized cyber-governance structure, yet many cyberattacks and influence campaigns are conducted by proxies such as the St. Petersburg-based Internet Research Agency.[54]

Yevgeny Prigozhin, a businessman linked to Putin, was the primary funder of the Internet Research Agency. The United States charges that Prigozhin purchased computer server space in the country, created fictitious personas, and stole identities of actual Americans in the effort to influence the 2016 presidential election.[55] Prigozhin leads the Wagner Group, a proxy organization for the Russian state known for malign operations in Central African Republic, Libya, Mali, Mozambique, Syria, Sudan, and Ukraine.

The United States and the European Union sanctioned the Wagner Group for "destabilizing activities" such as fake election monitoring and other information operations, and "serious human rights abuses, including torture and extrajudicial, summary or arbitrary executions and killings, or in destabilizing activities in some of the countries they operate in."[56] The Russian government denies involvement.

Operating from a weaker position, Russia employs a "raiding" strategy, harassing the United States and making territorial gains in the former Soviet sphere of influence.[57] Russia uses Estonia, Georgia, and Ukraine as testing ranges for cyber weapons. In January 2022, amid rising tension including 100,000 Russian troop deployments on the border of Ukraine, a destructive malware appeared in Ukraine government computers, defacing the websites. Microsoft identified a malware that poses as ransomware and when activated, is capable of destroying files and wiping hard drives.[58]

Russia ramped up its social media campaign encouraging Russian speakers within Ukraine to support military action. Meanwhile, a US official warned of a possible

53. IISS, "Net Assessment," 104.

54. IISS, "Net Assessment," 103.

55. FBI Counterintelligence, "Yevginiy Vicktorovich Prigozhin3.pdf," Most Wanted (website) n. d., accessed January 16, 2022, https://www.fbi.gov/.

56. "EU Sanctions Target Russian 'Wagner' Mercenary Group," Deutsche Welle, December 13, 2021, https://www.dw.com/.

57. Michael Kofman, "Raiding and International Brigandry: Russia's Strategy for Great Power Competition," War on the Rocks, June 14, 2018, https://warontherocks.com/.

58. David E. Sanger, "Microsoft Warns of Destructive Cyberattack on Ukranian Computer Networks," *New York Times*, January 16, 2022, https://www.nytimes.com/.

Russian "false flag" operation, involving Russian sabotage of its own allies within Ukraine, as a pretext to invade.[59]

Russian Army Chief of Staff Valery Gerasimov emphasizes roles for information, cyberwarfare, propaganda, and deception. "The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness."[60] Russia uses civilian proxies, unidentified local and Russian agents, bribery, intimidation, agitation, assassination, and denial of operations.[61]

Russia's information confrontation has two faces: (1) information-technical, or cyber—networks, exfiltration, and infrastructure; and (2) information-psychological—operations that aim to influence, sow doubt, erode faith in public institutions, erode the will to fight, divide, and debilitate. The SolarWinds hack in 2020, attributed to the Russian intelligence service (SVR), is an example of the former.[62] SolarWinds compromised thousands of Americans as well as many government entities including the Departments of Defense, Treasury, Justice, and Energy, and the Cybersecurity and Infrastructure Security Agency.

Russia used both technical and psychological approaches to interference in the US 2016 election. [63] Russia conducted technical "computer-intrusion operations" against election infrastructure and the campaign of Hillary Rodham Clinton. Russian information—psychological operations included the release of the documents and other direct engagement with Americans.[64] In 2016, Russians purchased at least 3,500 ads on Facebook. Many ads and posts by Russian trolls or bots disguised the identity of the persona.[65] Russian trolls studied American perceptions, motivations, stressors, and attitudes to identify vulnerabilities and susceptibility to influence. A fake "Army of Jesus," for example, targeted religious American audiences.[66] The Internet Research Agency stoked antagonism on both sides prior to the ultimately deadly political rally in Charlottesville, Virginia in August 2017.[67]

---

59. Brooke Singman, "Russia Preparing False-Flag Operation as Pretext for Ukraine Invasion, US Warns," Fox News, January 14, 2022, https://www.foxnews.com/.

60. Valery Gerasimov, "The Value of War Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations," *Military Review* (January-February 2016): 24.

61. *Little Green Men: A Primer on Modern Russian Unconventional Warfare, Ukraine, 2013–2014,* unclassified vers. (Fort Bragg, NC: United States Army Special Operations Command, 2015).

62. Dina Temple Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of the SolarWinds Hack," All Things Considered, National Public Radio, April 16, 2021, https://www.npr.org/.

63. Robert S. Mueller, III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election,* vol. I (Washington, DC: USDOJ, March 2019), 1, https://www.justice.gov/.

64. Scott Shane, "How Unwitting Americans Encountered Russian Operatives Online," *New York Times*, February 18, 2018, https://www.nytimes.com/.

65. Guadagno and Guttieri, "Fake News."

66. Parlapiano and Lee, "Propaganda Tools."

67. Michael Martelle, ed., *Exploring the Russian Social Media Campaign in Charlottesville*, National Security Archive, The Cyber Vault Project, February 14, 2019, https://nsarchive.gwu.edu/.

Assessing Strategic Competition

To paraphrase Carl von Clausewitz, the most important judgment is to know the kind of war one is in.[68] United States strategy documents articulate a contest of deterrence, sustaining the international order by threat of punishment.[69] Accordingly, the Air Force has invested in technology to create ever more sophisticated and connected systems to amplify the speed, stealth, precision, and deadliness of that punishment.

By contrast, China and Russia, as challengers, seek advantages in a gray zone contest without triggering that punishment. In doing so, both have embraced the more holistic and original US conception of information warfare—both information-technical and information-psychological. Russia developed digital tools to super charge Soviet-era agitation tactics in "information confrontation."[70] China developed an integrated cyber-information framework of informatized warfare. This broader information-warfare concept has recently experienced a revival in the American strategic conversation.

In a 2019 study, Joshua Sipper and I identified four trends fueling this revival: (1) the ubiquity of cyberspace and accompanying technologies in everyday life; (2) a maturation of capabilities including the ability to kill; (3) a recognition of the interrelatedness of information-related capabilities including electronic warfare, and cyber, intelligence, psychological, and information operations; and (4) the offensive advantage and the development of offensive cyber operations policy and doctrine.[71] Are these trends sufficient to prompt innovation?

Accelerate Change

Those who study military innovation look for change, "in the goals, actual strategies, and/or structure of military organization."[72] A major innovation as defined by Rosen is "change in one of the primary combat arms of a service in the way it fights."[73] Innovation may take the form of redefining goals, a change in the concept of operations, or even the creation, as with the US Space Force in 2019, of a new combat arm.

The Air Force has not created a cyber force, nor was it a favorable indicator when, in 2021, the Air Force dropped "cyberspace" from its mission statement. At that time,

68. Carl von Clausewitz, *On War*, 8th ed., ed. and transl. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 88.

69. Joseph R. Biden Jr., *Interim National Strategic Guidance* (Washington, DC: White House, 2021).

70. Lesley Kucharski, *Russian Multi-Domain Strategy against NATO: Information Confrontation and Forward-Deployed Nuclear Weapons in Europe*, Center for Global Research, Lawrence Livermore National Laboratory, February 2018, https://cgsr.llnl.gov/; and Thomas Rid, *Active Measures*, 1st ed. (New York: Farrar, Straus & Giroux, 2020).

71. Karen Guttieri and Joshua Sipper, "Why It's All about Information Warfare Now," (paper presented at the NATO at 70 Conference, Troy University, Troy, AL, November 2019).

72. Theo Farrell and Terry Teriff, "The Sources of Military Change," in *The Sources of Military Change*, ed. Theo Farrell and Terry Terriff (Boulder, CO: Lynne Rienner, 2002).

73. Rosen, *Next War*, 7.

the Air Force mission statement changed "Fly, fight and win . . . in air, space and cyberspace," to "Fly, fight, and win – airpower anytime, anywhere." This rewording eliminates cyber and space. The Air Force was returning to its "core" mission.[74] Military innovation may require change not only in operations, but in culture.

The Air Force and the United States in general did make numerous institutional changes in response to perceived changes in the security environment. But if innovations "that change the context within which war takes place" are "the most influential," the Air Force must accelerate change in force development, preparing and promoting an officer corps to envision and execute a new way of war.[75]

In 2010, the United States established Joint US Cyber Command and in 2011 recognized cyberspace as a warfighting domain alongside land, sea, air, and space.[76] That was "liberating," wrote Michael V. Hayden, but it was significant that this domain was "a creation of man" and he wondered whether the possibilities it opened up were enough to "rethink" doctrine.[77]

United States Cyber Command's modest initial concept was to support conventional forces in crisis and sustain the ability to respond to significant attacks on US critical infrastructure. By 2012, that was no longer sufficient.[78] Cyber Command established a cyber mission force, "ready to execute a range of cost-imposing operations."[79] Today the Air Force provides 40 percent of the 133 teams that compose this force.[80]

Although the Air Force did not create a separate force for information warfare, it did create a new numbered Air Force for information warfare. In 2019, the Air Force combined the numbered Air Forces for intelligence and cyber to create the Sixteenth Air Force for information warfare. A single lieutenant general represents intelligence and cyber on the Air Staff.

---

74. Joshua Dewberry, "Air Force Unveils New Mission Statement," US Air Force News (website), April 8, 2021, https://www.af.mil/.

75. Alan R. Millet and Williamson Murray, *Military Innovation in the Interwar Period*, 1st paperback ed. (Cambridge: Cambridge University Press, 1998), 305.

76. David Alexander, "Pentagon to Treat Cyberspace as 'Operational Domain,' " Reuters, July 14, 2011, https://www.reuters.com/.

77. Michael V. Hayden, "The Future of Things 'Cyber,'" *Strategic Studies Quarterly* 5, no. 1 (Winter 2011): 4.

78. Paul M. Nakasone, "A Cyber Force for Persistent Operations," *Joint Force Quarterly* 92 (1st Quarter 2019): 11, https://ndupress.ndu.edu/.

79. *Testimony to Subcommittee on Intelligence and Emerging Threats and Capabilities, Hearing before United States Congress House of Representatives, Committee on Armed Services*, 116th Cong. (March 4, 2020) (statement of General Paul M. Nakasone, commander, US Cyber Command, and director, National Security Agency), https://www.congress.gov/.

80. Mark Pomerleau, "Air Force Would Contribute Bulk of New Cyber Mission Force Teams," DefenseNews, July 14, 2021, https://www.defensenews.com/.

In 2020, Nakasone declared the top priority for US Cyber Command was to ensure the US election was "safe, secure, and legitimate."[81] A military structure focused on cyberspace protecting democracy at home would have been difficult to imagine not so long ago. Also in 2020, Cyber Command and Microsoft mutually responded to Trickbot, although the degree of coordination remains unclear. Trickbot, a botnet of over one million infected servers attributed to Russian criminals, was connected to ransomware against hospitals and threatened US systems for the 2020 election.[82]

Cyber Command hacked into the botnet servers and replaced exposed passwords and financial data with junk data to make them useless. Microsoft obtained a federal court order and took its own servers offline in order to thwart the botnet.[83] Meanwhile by November 2021, Cyber Command had conducted over a dozen "hunt-forward" operations, which can be offensive in nature, and had done so in fourteen countries in recent years.[84] Teams from the United States in Ally and partner nations spot adversary operations and share the information with partners.

After returning to the drawing board on the Joint warfighting concept, Hyten noted the goal is to be "fully connected to a combat cloud that has all information that you can access at any time, any place . . . to be able to act quickly on that."[85] He described expanded maneuver in space and time, aggregation for lethality, and disaggregation for survival with more secure, just-in-time information. It will require officers to make it so.

Developing Airmen for Information Warfare

A new way of war ascends with officers who are learning and practicing it; developing and promoting these officers is a long-term investment. Promotion matters because change agents make certain enemies and uncertain friends, therefore strong leadership is needed to shelter creative thinkers.

The US Army Air Forces in the 1940s made the argument that they did not only support other warfighters, they created strategic effects. "If talented cyberwarriors convince themselves that strategic warfare offers a better slot at top command slots, they will migrate accordingly. Perhaps if cyberwar is that important, there will be

81. Sydney J. Freedberg Jr., "2020 Elections: NSA and Cyber Leader is Confident vs. Russia" Breaking Defense, July 20, 2020, https://breakingdefense.com/.

82. Jay Greene and Ellen Nakashima, "Microsoft Seeks to Disrupt Russian Criminal Botnet It Fears Could Seek to Sow Confusion in the Presidential Election," *Washington Post*, October 12, 2020, https://krebsonsecurity.com/.

83. Brian Krebs,"Microsoft Uses Trademark Law to Disrupt Trickbot Botnet," KrebsonSecurity (blog), October 12, 2020, https://krebsonsecurity.com/2020/10/.

84. Brad D. Williams, "Cybercom Has Conducted 'Hunt Forward' Ops in 14 Countries, Deputy Says," Breaking Defense, November 10, 2021, https://breakingdefense.com/.

85. David Vergun, "DOD Focuses on Aspirational Challenges in Future Warfighting," US Department of Defense News (website), July 26, 2021, https://www.defense.gov/.

enough resources and manpower to go around."[86] The Air Force must open paths forward for both people and ideas.

The Trickbot scenario, with legal issues and public-private operations, offers a good example of the unique complexities of information warfare. Securing US elections requires strategic integration of operational expertise and extensive coordination across and within government, military, private sector, and international partners. Thwarting terrorist propaganda online for recruiting and financing takes technical expertise plus leadership and campaign-planning skills. Without question, "recruiting, training, developing, and retaining the best talent is essential for the military to defend the Nation in cyberspace."[87] This is the responsibility of the services, but each is already preoccupied with their respective domain.

The executive director of the bipartisan Cyberspace Solarium Commission and his coauthors argued "each of the services should be offering significant programs in cyber strategy at their war colleges."[88] The commentary lamented that the dedicated cyber strategy programs that did exist were under constant threat of extinction.

Lieutenant General Mary O'Brien, Air Force deputy chief of staff for Intelligence, Surveillance, Reconnaissance and Cyber Effects Operations, issued an "integration imperative" of previously compartmentalized information warfare capabilities.[89] Information technology skills alone will not meet this intent. First, when new skills are associated with a technical specialty, those officers are in danger of being "relegated to professional oblivion."[90]

Second, integration implies an interdisciplinary curriculum. In addition to using technology, officers must "leverage information effectively to shape relevant actor behaviors, perceptions, and attitudes."[91] The emerging field of social cybersecurity has much to offer in complement to technical training. This field focuses on the intersection of human behavior and technology, including how cyber mediates "changes in individual, group societal, and political behaviors and outcomes." Applied work supports "building of the cyber infrastructure needed to guard against cyber-mediated threats."[92] Human factors in cyberattacks—how threat actors use cyberspace to recruit and finance operations, mobilize extremists to action, and sway elections—must be analyzed.

---

86. Libicki, *Peace and War*, 166.

87. Nakasone, "Testimony."

88. Erica Borghard, Mark Montgomery, and Brandon Valeriano, "The Challenge of Educating the Military on Cyber Strategy," War on the Rocks, June 25, 2021, https://warontherocks.com/.

89. Mary F. O'Brien, *Integration Imperative: Synchronization of Information Warfare Functions* (Washington, DC: Department of the Air Force, 2021).

90. Rosen, *Next War*, 20–22.

91. O'Brien, *Integration Imperative*.

92. National Academies of Sciences, Engineering, and Medicine 2019, *A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis* (Washington, DC: The National Academies Press, 2019), 142, https://doi.org/.

Commander of Air Combat Command General Mark D. Kelly observes, "while there are many Air Force and DoD programs currently available to build essential technical cyber skills, the Air Force cannot afford to passively await the development of cyber strategists by happenstance or on-the-job training of those already filling critical positions."[93] Currently, force development stalls out beyond cyber hygiene, digital literacy, and IT training. For select Airmen, the service offers training in digital forensic analysis, intrusion-detection response, and other sophisticated technical skills. As important as those *cybersecurity* skills are, the Air Force also needs cyber *strategy* skills to accelerate change.

And Win

Should the Air Force fail to innovate, General Brown's prognosis is grim: "If we don't change—if we fail to adapt—we risk losing the certainty with which we have defended our national interests for decades. We risk losing a high-end fight. We risk losing quality Airmen, our credibility, and our ability to secure our future."[94] Persistent engagement in cyberspace has created a new context and roles for Brown's Air Force.

To win the information war, the Air Force will need tech-savvy leaders and strategists. These officers must be able to partner constructively with other US agencies and industry players and Ally and partner nations. The Air Force can accelerate change if it invests not only in technology but also in the leaders needed to conceive and fight this new way of war. *Æ*

Karen Guttieri, PhD
Dr. Guttieri is the dean of the Air Force Cyber College.

93. Mark D. Kelly, "Requirement for Air Force Cyber College Programs," (Washington, DC: Department of the Air Force, August 2, 2021).

94. Brown, *Accelerate Change*, 2.