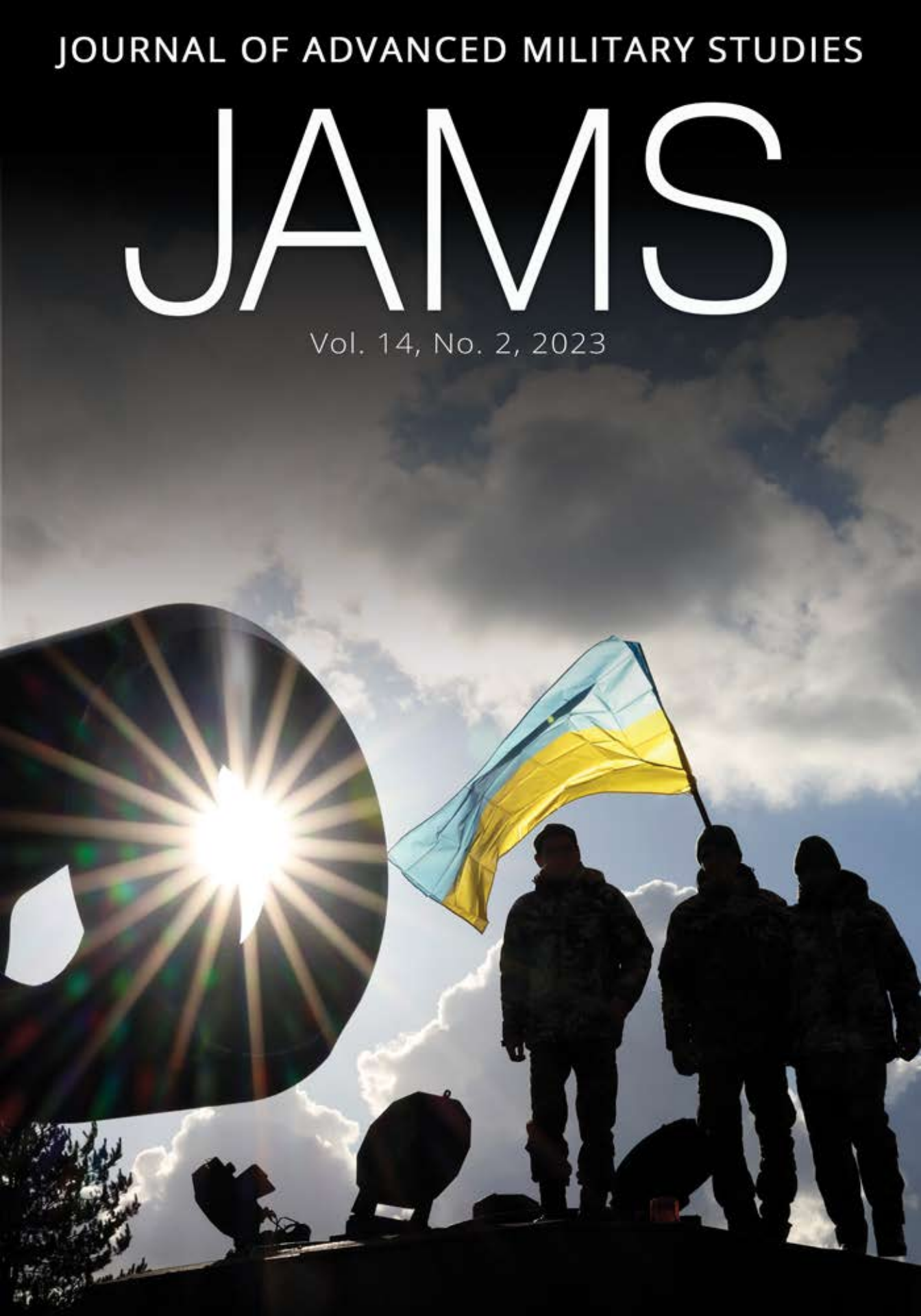
JOURNAL OF ADVANCED MILITARY STUDIES

JAMS

Vol. 14, No. 2, 2023



Journal of Advanced Military Studies
(Print) ISSN 2770-2596
(Online) ISSN 2770-260X

Established in 2008, MCU Press is an open access publisher that recognizes the importance of an open dialogue between scholars, policy makers, analysts, and military leaders and of crossing civilian-military boundaries to advance knowledge and solve problems. To that end, MCUP launched the *Journal of Advanced Military Studies* (JAMS) to provide a forum for interdisciplinary discussion of national security and international relations issues and how they have an impact on the Department of Defense, the Department of the Navy, and the U.S. Marine Corps directly and indirectly. JAMS is published biannually, with occasional special issues that highlight key topics of interest.

ARTICLE SUBMISSIONS

The editors are looking for academic articles in the areas of international relations, geopolitical issues, national security and policy, and cybersecurity. To submit an article or to learn more about our submission guidelines, please email MCU_Press@usmcu.edu.

BOOK REVIEWS

Send an email with a brief description of your interests to MCU_Press@usmcu.edu.

SUBSCRIPTIONS

Subscriptions to JAMS are free. To join our subscription list or to obtain back issues of the journal, send your mailing address to MCU_Press@usmcu.edu.

ADDRESS CHANGE

Send address updates to MCU_Press@usmcu.edu to maintain uninterrupted delivery.

INDEXING

The journal is indexed by ProjectMUSE, Scopus, ScienceOpen, EBSCO, ProQuest, Elsevier, OCLC ArticleFirst, Defense Technical Information Center, Journal Seek, IBZ Online, British Library System, Lancaster Index to Defense and International Security Literature, and AU Library Index to Military Periodicals.

FREELY AVAILABLE AT
WWW.USMCU.EDU/MCUPRESS

Contents

Vol. 14, No. 2

BOOK REVIEWS

The Cold War Computer Arms Race

Captain Bryan Leese, USN, PhD

Abstract: The Cold War computer arms race illustrates the military's role in strategic competition. The Soviets bought and stole, versus creating computer technology themselves. A U.S.-led coalition integrated economic, diplomatic, and information mechanisms, embargoing computer technology to disadvantage the Soviets. President Ronald W. Reagan's offset strategy integrated military power, openly demonstrating computer-infused weapons lethality that jeopardized Soviet quantitative military advantage. President Reagan's use of the computer arms race shows a way to conduct and integrate a strategic competition campaign of deterrence that includes coercive diplomacy with diplomatic efforts that can deter China and Russia while encouraging them to reverse harmful foreign and domestic policies.

Keywords: Cold War, competition, computers, deterrence, coercion, technology, embargo, industrial espionage

In 1992, former assistant secretary of defense Leslie H. Gelb recalled an off-the-record conversation with Chief of the Soviet General Staff Marshal Nikolai V. Ogarkov that had taken place in 1983. The plainspoken, hardline general of the Soviet state made it clear that, in his opinion, the Cold War was essentially over. In Ogarkov's mind, Gelb recalled, the West had won because

> [The] numbers of [Soviet] troops and weapons mean little, he said. We cannot equal the quality of U.S. arms for a generation or two. Modern military power is based upon technology, and technology is based upon computers. In the U.S., he continued, small children—even before they begin school—play with computers. Computers are everywhere in America. Here, we don't even have computers in every office of the

Capt Bryan Leese is a career intelligence officer and former military professor in the Joint Military Operations department at the U.S. Naval War College. He holds a master's in strategic studies from the U.S. Army War College and a PhD in war studies from King's College London. https://orcid.org/0009-0001-7043-6235.

> Defense Ministry. And for reasons you know well, we cannot make computers widely available in our society. Then came his portentous punch line: We will never be able to catch up with you in modern arms until we have an economic revolution. And the question is whether we can have an economic revolution without a political revolution.[1]

Ogarkov recognized that within the competition that defined the Cold War, the Soviets had lost the computer arms race to the United States. Without computers, no number of men or weapons could overcome the United States' asymmetrical technologic advantages.

This article examines the competition over computer technology during the Cold War. It highlights the importance of technology in shaping competitive strategies and illustrates some of the military's role in a successful, integrated strategic competition campaign. The Cold War computer arms race provides context for current and future competition with China and Russia.

The Problem

Ogarkov's Cold War observation regarding competition is prescient today. Seeing peace and war as binary conditions does not help us understand the great power competition (GPC) with China and Russia. Peace does not exist, just the absence of war. Competition, some cooperation, and the fear of a possible conflict are the reality. The U.S. Joint force is shifting to a strategic competition paradigm that better fits today's reality by leveraging its dominance in the technology arena.[2] However, the United States' technical superiority in conventional and nuclear weapons has lessened. China is now considered a peer military threat.

The United States is increasing its emphasis on research and development of artificial intelligence and autonomous unmanned weapons systems, among other technologies, to grow the capabilities gap between it and China. At the same time, the United States must control technology transfer to slow China, Russia, and others. But the U.S. defense acquisition system is seen as too slow and its controls too weak. Even its recent efforts, like the Adaptive Acquisition Framework, to speed up weapon system development and deployment have yet to significantly increase the United States' technological comparative advantage.[3] China's technology and weapon systems development keeps pace by supplementing its efforts with academic and economic espionage.

A recent *New York Times* article reported a multiyear FBI investigation exposing a pervasive, systematic, and vast "economic espionage offensive . . . waged unilaterally by China" against U.S. military technology companies.[4] Economic and academic espionage is a strategic competition mechanism, leveraging theft to shorten technology development and fielding time lines. The technologically advanced side's desire to manage competition escalation through cooperation often makes theft possible. Finding ways to cooperate on a narrow set of common interest areas, like medical technologies or fighting climate change, re-

duces pressure in military and economic competition areas prone to escalation. However, the cooperation aids in technology transfer and theft.

Today's Chinese industrial espionage appears eerily like the Soviet Union's during the Cold War. As seen with détente, the United States' desire to use academic and economic cooperation created Soviet access to dual civilian and military use technologies. And the Soviets, like the Chinese today, benefited especially from access to the computer and digital technologies. The United States' technology dealings with China in the twenty-first century seem to have forgotten the 1970s and 1980s Cold War computer arms race lessons.[5]

The Cold War Computer Competition Begins

Following the Second World War, the U.S. Navy reflected on the difficulty of air defense battle management during Japanese kamikaze air attacks. They realized that air defense in the jet age was untenable without automation. The Navy blended technologies from cryptography, analog gunnery computers, and the calculation of ballistic missile trajectories to create a series of information management computers called the Naval Tactical Data System (NTDS) for air battle management.[6]

At the same time, the U.S. Air Force worked to create an integrated early warning and national air defense battle management system called the Semi-Automatic Ground Environment (SAGE). NTDS and SAGE developed intercomputer and teletype datalinks, improving human-to and computer-to-computer interaction. The two programs forged links with military research laboratories, commercial industry, and academic institutions that developed, built, and evolved computers. Throughout the 1950s, the collaboration produced the transistor, the integrated circuit (computer chip), the printed circuit card, and the Univac series of computers. The continually miniaturized computers using newly developed materials and techniques made them fit into ships and aircraft.[7] The civilian-academic-military development provided technologies that International Business Machines Corporation (IBM), Control Data Corporation (CDC), and Honeywell adapted for commercial business and industry use.

In 1959, the Department of Defense created the Advanced Research Projects Agency (ARPA) to exploit advanced ballistic missile defense and nuclear test detection technology. The space mission shifted to the newly created National Aeronautics and Space Administration (NASA). ARPA focused on computer "internetting" (or what we call networking today) technology.[8] Networking computers increased the overall computing power available and allowed data sharing. The 1962 Cuban missile crisis showed that the inability to share data across the national and military command and control (C2) systems almost resulted in a nuclear weapons conflict. The 1960s effort to consolidate and internet C2 systems created the Worldwide Military Command and Control System (WWMCCS, pronounced Wimex).

The theory critical to the success of networking was "distributed commu-

nication," proposed by Paul Baran at Rand in the early 1960s.[9] The human brain, Baran observed, overcame damage to the neural network by rerouting messages across its distributed pathways. He argued that a computer network could do the same by breaking messages into many blocks. Each block had an identity or handover code and destination address. The blocks were stored and forwarded through the "shortest instantaneously available path through the network." Baran dubbed the store and forward approach as "hot-potato" heuristic routing. As the blocks arrived, the message was reassembled using the handover code.[10] ARPA's network project (ARPANET) focused on expanding computer time-sharing using distributed communication networks.[11]

Baran widely published his research and simulations. His concepts were radical, disruptive thinking that challenged the current voice and data transmission approach. It took several years before the concepts were adopted.[12] Finally, on 29 October 1969, two computer nodes, one at Stanford Research Institute (SRI), Menlo Park, CA, and another at UCLA's Boelter Hall, Portola Plaza, Los Angeles, CA, some 563 kilometers apart, were able to internet. Today's World Wide Web (WWW), a global system of interconnected computer networks, was born with the simple networking of those two computers.

In the 1970s, 80s, and 90s, the U.S. and Western computer industries produced more and more computers, making them smaller, more powerful, and more connected. The West's computer industry validated the increasing rate of technology growth that Gordon E. Moore, the cofounder of Fairchild Semiconductor and Intel, posited in 1965.[13] In the Soviet Bloc, however, the computer industry lagged and struggled.

Soviet Cybernetics Development

Computer science theories, called cybernetic theories in the post–Second World War era, were pitched to top Soviet party leaders and condemned as a capitalist plot.[14] Soviet military and economic planners, however, recognized the need for computers. It was a conundrum Ogarkov alluded to in his 1983 statement to Gleb. In classic Soviet doublespeak, the Soviets secretly pursued military computing while "condemning the West for doing the same."[15]

After the death of Joseph Stalin in 1953, cybernetics slowly returned to the academic institution and Russian industry. Nikita Khrushchev broke with Stalin's isolationism in the mid-1950s. Khrushchev felt that Stalin had culled many specialists needed to grow the economy. Under his de-Stalinization policy, Khrushchev somewhat liberalized society and reformed the Soviet industrial infrastructure. The problem with the economy, Khrushchev believed, was the oppressive centralization of its management. His policies looked to undo the party hierarchy by promoting specialists and creative thinkers above long-term party members.[16]

Khrushchev's new policies had some initial success. The sale of consumer goods grew and so did the Soviet economy. Increased weapons sales to the Third World improved the economy while increasing Soviet influence and spreading

Communism. Budget reductions were also needed, and Khrushchev cut military manpower by 5.7 million from 1956 through 1957. He also increased the production of new technologies. Even with these changes, by 1959, the optimism that the Soviet economy would "bury" capitalism, as Khrushchev had exclaimed at a 1956 embassy reception in Moscow, was fading inside the party.[17] Khrushchev believed he needed to decentralize economic policy making further. He removed the planning from the Kremlin, pushing it down to regional economic planning subcommittees. However, decentralization only works if the regional subcommittees share production and economic planning data. To do so required using cybernetics, the computers and integrated networks that Stalin had been against.[18]

The widespread administrative decentralization was anathema to the Soviet system. University of Tulsa professor Benjamin Peters argued that the decentralization contributed to the derailment of the Soviet cybernetic efforts. By marginalizing many party officials, the decentralization "further contribute[d to] the disarray and discontent associated with his [Khrushchev's] leadership." By the 1962 Cuban crisis, the Soviet national economy remained lethargic, and the "information management behind its planning were proving increasingly inadequate."[19] Disenfranchised top-party members took every opportunity to derail decentralization and the effort to "carry out wide-scale cybernetic structural reforms." Seeing that his reforms were not working, Khrushchev found that decentralization left him "without the control over the very reforms he wished to enact."[20] Though the Russian cyber science that led the cybernetic structural reform effort was solid, Peters argues, its demise was due to the unregulated internal competition between top party leaders for primacy.[21]

Like the Americans, the Soviet military used computers to improve strategic warning and decision-making. Unlike the American's Wimex, the Soviet military created three separate warning and C2 networks for air defense, missile defense, and space surveillance. The three Soviet systems tried to match the centralized U.S. Air Force's SAGE. However, they chose instead to develop three unconnected systems.[22] A 1972 U.S. national intelligence estimate (NIE) reported that the Soviet ballistic missile warning network provided only negligible capability and "show[ed] no prospect of becoming effective against a major attack." The air defense network was better, providing a "formidable defense." The space surveillance system could track and likely intercept orbital satellites.[23] Soviet cybernetics was a series of "stovepipe" efforts limiting the collaboration required for large-scale computer production and implementation.

Soviet military cybernetics innovator Anatoly I. Kitov's efforts to break the "stovepipes" illustrate the shortcomings of the Soviet's effort. In 1956, Kitov proposed an ARPANET-like nationwide internet network, though it differed in the details of its design. In a 1959 report meant to go directly to Khrushchev, Kitov recommended that the military share its information management systems to improve civilian economic planning through internet-connected computers. The military dismissed Kitov's recommendation, removed him as the

director of Computational Center-1 of the Ministry of Defense, and revoked his party membership for good measure.[24]

The Soviet system continued to privilege highly classified military cybernetic efforts by defense ministries and institutions while isolating efforts by the civilian sector. There was no governing body to force cybernetic cooperation between the organizations. Khrushchev's reform had unwittingly created ministries and institutions "not only unwilling to cooperate . . . [but] often in hostile competition with their peer institutions."[25] Thus, Soviet cybernetic theories grew slowly, but throughout the 1960s, their practical application and the creation of a civilian computer industry lagged behind the West's.

Buy and Steal

In the Spring of 1970, the Communist Party realized they required more and better computers to compete with the West. The State Planning Committee (Gosplan) released a five-year economic plan directing a 260 percent increase in computer production. The Soviet computer industry could never meet this demand. The small industry leaned heavily on the IBM/360 platform, pirating the design for their Ryad model computers. But the industry could not produce the quantities desired.

Since the Soviets could not build the numbers directed, they looked toward détente to buy Western computers. It was a fateful decision.[26] Historian Simon Doing offers that the Soviets chose as they did because the West's computers were better than anything the Soviets were making. By buying computers, the Soviet states unwittingly adopted American technology and its standards. The dominance of English language-based computer operating software allowed American programmers to set the de facto standard for the world.[27]

The Soviets throttled back on developing their computer production industry because the West seemed willing to fill the gap. Then, the Soviets discontinued most of their independent computer technology and industry development.[28] The Soviet's "take" approach was adequate if the West continued to sell them computers. The Soviets realized that the West might be unwilling to sell them computers at some point. Thus, they began an aggressive effort to steal the technology. The theft approach was not new.

As early as 1924, a steady stream of Soviet spies operating illegally under fake business or diplomatic credentials stole intellectual property from the West. By the 1980s, the Soviets had become experts at stealing industrial technology. The thefts occurred even during the Second World War when the Soviets, British, and Americans were allies.[29] Eugene S. Poteat, a senior Central Intelligence Agency (CIA) executive during most of the Cold War, wrote that the Soviet intelligence services stole "virtually all the West's military and defense technology secrets" in the post–Second World War era. The thefts saved the Soviets time and the expense of research and development; it allowed them to keep pace with the technology competition in the early days of the Cold War.[30]

The West had a growing concern about selling computers to the Soviets. By

1973, the West sought to strengthen the diplomatic and economic sanctions used since 1948 to slow technology transfer to the Soviet Bloc. The control measures forced the Soviets to always "play catch-up" to the West in technology. The embargo's trade controls were overseen by a consultative group of North Atlantic Treaty Organization (NATO) members and Japan called the Coordinating Committee for Multilateral Export Control (CoCom). There were more than 500 items embargoed from export to the Soviet Bloc and China. Embargoes are a double-edged sword; they also impeded the West's economic expansion.

Historian Frank Cain wrote that the embargo policy created a growing divide "between the UK and USA concerning whether the trade should prevail over ideology."[32] Keeping the allies and industry on the same side regarding the embargo was challenging. Britain disagreed with many export strictures and used "exception provisions" to justify to CoCom the sales of computers. Further, the Soviet Bloc's "general progress toward self-sufficiency" made some export controls seem obsolete. The list of export-controlled items and individual nations' requests for exemption to the list was in constant tension.[33]

Under détente, the strict export controls on the sale of computers lessened, replaced by a series of loose post-sale control mechanisms. National Security Advisor Henry Kissinger codified the "free trade with conditions" position and post-sale controls of the Richard M. Nixon administration in the March 1974 national security decision memorandum (NSDM) 247. The memorandum increased the maximum computer processing rate requiring special export licenses, simultaneously expanding and strengthening the "post-sale safeguards."[34] The safeguards were costly and extraordinary since they were executed on Soviet soil after export, a unique penetration of the closed Soviet state. The controls included on-site inspections by Westerners permanently based in the Soviet Union. Inspectors were authorized to scale down systems on-site if the computing power exceeded the agreed-upon requirement.[35] To Nixon, the controls were enough to maintain security and détente. Not everyone agreed.

Members of Congress perceived that selling technology to the Soviets eroded the United States' technological advantage, no matter the strictures used. A 1970 intelligence community memorandum regarding the CoCom countries' sales to the Soviet Bloc assessed a lessening of export control efficacy. The report, viewed through an alarmist lens, provoked further concern and analysis of détente-related trade relaxations.[36] A 1973 Rand report prepared for the Department of Defense and the Council on International Economic Policy offered that the computer gap between the United States and the Soviets had been reduced. The Soviets closed the gap by buying computers, conducting illegal technology transfers, and through industrial espionage.[37] None of the post-sale controls outlined by Kissinger was satisfactory to technology "protectionists" inside the military or Congress.

The United States feared the Soviets were catching up even when data countered the shrinking computer gap argument.[38] "Gap" theory, or the belief that an adversary has superiority in technology, weapons, and national power

compared to the United States, dominated U.S. strategic culture during the Cold War. Intelligence and defense communities hotly debated atomic weapons, bombers, and missile numbers.[39] While not as prominent as the weapons debates, the computer gap underpinned many technologies needed to develop and employ the weapons.

Trade issues with the Soviet Bloc came to the forefront in 1973. Nixon desired further reforms that opened trade, setting up a traditional domestic battle between "free trade" and "protectionist" groups.[40] Some protectionists in Congress claimed CoCom safeguards protected the use of the systems, not the transfer of technology.[41] The debate continued throughout 1974 and 1975. The transfer of tangible technology, the systems, leading to a loss of intangible knowledge, the know-how, to the Soviets was the foundation of the J. Fred Bucy-led panel's recommendation (the Bucy Report) in 1976. The report successfully advocated a conceptual shift from regulating physical goods to controlling know-how. The Bucy Report's primary concern was not reverse engineering; it rejected that concern as an ineffective way of technology transfer. The real fear was that the Soviets might acquire so much experience operating and maintaining cutting-edge technology that they learned how to design and manufacture the computers themselves.[42]

Computers Enhanced Warfare and Reagan's Strategic Competition

Ronald Reagan saw "peace through strength" as the only approach to dealing with the Soviets; he swept into power. His predecessor, President James E. "Jimmy" Carter, had a stagnant national security strategy that looked to maintain the status quo of détente. His strategy failed. In 1976, new Soviet SS-20 intermediate-range missiles were deployed, forcing NATO to take a "dual-track" response. NATO negotiated the removal of the SS-20s while planning to deploy Pershing II and a ground-launched cruise missile (GLCM) version of the Navy's Tomahawk.[43] The year 1979 became a year of crisis as the Soviets invaded Afghanistan, the Shah of Iran was overthrown, American hostages were seized in Tehran, and the socialist Sandinistas came to power in Nicaragua. Carter increased defense spending by around $8 billion ($32.6 million in 2022 dollars), focusing money on the technology-based offset strategy begun in 1972. Nevertheless, it was too late.[44]

In 1981, Reagan reinvigorated the 30-year-old containment strategy and integrated it with more aggressive competition. By 1983, Reagan's strategy was formed and in operation. Security Decision Directive 75 expressed his intention to "contain and over time reverse Soviet expansionism by competing effectively on a sustained basis with the Soviet Union in all international arenas."[45] The United States would compete across a variety of security areas. Competition would include nuclear and conventional weapons development and employment using openly discussed war fighting strategies, economic sanctions, promotion of human rights, and efforts to undermine Soviet advancements in the

Third World by using open and covert support for anti-Soviet resistance movements in Eastern Europe, Afghanistan, Angola, Ethiopia, and Nicaragua.[46]

Reagan started by emphasizing the expansion of U.S. military forces. He asked for an increase of $43.4 billion in defense spending.[47] Expanding the force and making it more capable created symmetry and restored the military balance with the Soviets, an essential mechanism for deterrence. It also allowed for U.S. military "action across the entire spectrum of potential conflicts."[48] By preparing for conflict, the military provided a foundation of deterrence and coercion that countered Soviet competition, allowing the full range of U.S. and Western policies to be used against the Soviet Bloc.[49]

However, increasing the military only mattered if the United States was willing to use the force. Removing the self-imposed post-Vietnam restrictions regarding the use of military force was Reagan's next goal. The willingness to use military power to achieve limited objectives that resulted in greater political ones was vital.[50] Reagan employed military force at least five times during his two terms in office.

Each time he used force, Bruce W. Jentleson argues, it was part of a broad coercive diplomacy effort. The use of force strategy "was more than deterrence but less than a quick, decisive military" outcome, Jentleson wrote, a methodical approach to force foreign policy restraint on the Soviets. For example, the CIA covertly supported Afghanistan mujahideen against the Soviet invasion. Conversely, the U.S. Marines deployed to Lebanon with the Multinational Force (MNF) in 1982–84. The Navy pressured Libya and eventually conducted a bombing in 1986. The Navy again was used in the 1987–88 reflagging of Kuwaiti oil tankers in the Arabian Gulf and the attack on Iranian naval forces.[51]

Short, sharp conflicts, like the invasions of Grenada (1983) and Panama (1989), and the display of new military technologies increased the perception of the lethality of U.S. military power. It supported the deterrence and coercive diplomacy effort.[52]

The U.S. military's technological advantage gave Reagan an asymmetric offset in the military power competition. Détente had shrunk the computer gap, lessening the U.S. military's offset strategy. For Reagan, détente was dead. He restored and increased controls over technology transfers and sales to the Soviet Bloc. More critical technologies and equipment were added to the CoCom embargo list, and national licensing procedures were changed to increase the effectiveness of enforcement efforts. Additionally, the United States began to unilaterally place export restraints on technology and equipment beyond the CoCom structure. In particular, the United States unilaterally embargoed computer technology associated with gas and oil production to impede Russia's petroleum-based economy.[53]

There were vulnerabilities inside the growing, almost ubiquitous application of computer technologies. It was not enough to use embargoes to restrict transfers yet leave the computer networks themselves vulnerable. Since 1972, the National Security Agency (NSA) warned that the current computer internet

technology and policies were inadequate. For example, there was no separation of classified and unclassified networks, NSA and the Air Force noted, and users without clearances worked at the same consoles as those accessing classified data. The dual-use consoles were more convenient and saved time, but they created a significant risk of "accidental disclosure."[54]

In the early-1980s, revelations about U.S. information security and command and control systems weakness came to light. Soviet economic and military espionage was more extensive than previously understood. In 1981, KGB (*Komitet Gosudarstvennoy Bezopasnosti*) science and technology collector and informant for the French intelligence service, Vladimir Vetrov (code name Farewell), provided a list of KGB targets and the extent to which industrial espionage had penetrated U.S. and Western technology industries.[55] Geoffrey Arthur Prime, a British Government Communications Headquarters employee, was arrested in 1982. Retired U.S. Navy chief warrant officer John A. Walker was arrested in 1985. The arrests revealed that for at least two decades, defense secrets were stolen from the information systems; it drove home information network security concerns.[56]

If the espionage unearthing was not enough, an incident in 1979 showed that data stored on a network could be manipulated, causing confusion that could lead to war. Someone at North American Aerospace Defense Command (NORAD) inadvertently entered nuclear weapons attack simulation data. A missile attack warning was sent from the computer, and a short, sharp panic ensued before the alert was canceled. But little would be done to secure U.S. military networks until the 1983 movie *WarGames* was released. The movie's premise was that a high school student deliberately hacked a Department of Defense computer, almost starting a global thermonuclear war. The movie inspired actions in the real world. A few high school students in Wisconsin hacked into unclassified Department of Defense computers that same year. Reagan acted quickly, creating policies and strictures that secured vital Department of Defense computers. Legislation, in the form of the Computer Security Act, would not catch up to policy until 1987.[57]

Reagan continued to leverage the U.S. military to create force legitimacy by openly discussing conventional weapons development and employment strategies to defeat Warsaw Pact forces. The approach added a new narrative dimension to the competition. The United States was so confident in its technology overmatch, so went the narrative, that it was willing to reveal some of its capabilities. The capabilities, and unifying thinking regarding how to use them, are expressed through military doctrine.[58] For example, the AirLand Battle doctrine promulgated in 1982, and later, the new maritime strategy revealed in 1986 influenced how the United States and NATO thought of and planned-for war against Warsaw Pact land forces in Europe.[59]

New U.S. military doctrine embraced emerging technologies that increased after the 1973 Yom Kippur War. Combined with the lessons from the Vietnam War, the Yom Kippur War reinforced the necessity of air power in conduct-

ing modern land warfare. The Soviets had drawn the same lesson. They began modernizing their military in the late 1960s. Throughout the 1970s, the Soviets developed a concept of strategic operations using conventional force in Europe. The Warsaw Pact ground forces would attack in depth using initial and reinforcing echelons. The initial attacking units, operational maneuver groups, penetrated NATO defenses while the follow-on echelon exploited the breakthrough.[60]

AirLand Battle was at the end of a doctrinal evolution addressing a series of technological improvements in both maneuver and reconnaissance-to-strike complexes. The improvements focused on attacking Soviet armor units in the initial and follow-on echelons to delay, disrupt, and destroy them before the Soviet Army could mass irresistible combat power. The U.S. Army would handle defeating the initial attacking units and the Air Force the follow-on echelons. AirLand Battle looked to exploit the perceived Warsaw Pact weakness of tactical rigidity, predictable echelonment, and technological inferiority.[61]

AirLand Battle doctrine drove an explosion in computer technology integrated battlefield systems development and procurement. The Air Force's battlefield air interdiction mission against follow-on forces led to the development of several standoff attack systems: the General Dynamics–Grumman EF-111 Raven standoff-jamming and reconnaissance platform, the laser-guided antitank Maverick air-to-surface missile, the McDonnell Douglas F-15 Eagle's beyond-visual-range radar missiles, and the specifically designed close-air-support tank killer, Fairchild Republic A-10 Thunderbolt II.[62] Despite the Air Force's deep battle systems development, the Army also developed the highly maneuverable Boeing AH-64A Apache helicopter. The Apache could attack the initial echelon and follow-on forces using its advanced weapons targeting system with a 20-mm chain gun and laser-guided Hellfire missiles to attack troops and armor. They also developed the MGM-140 Army Tactical Missile System (ATACMS). With a 306-kilometer range, the surface-to-surface missile ATACMS fired antipersonnel and antiarmor submunitions from a mobile multiple-launch rocket system.[63]

Probably the most significant weapon system developed was the Assault Breaker demonstration program. Assault Breaker integrated several technologies developed during and after the Vietnam War, including lasers, electro-optical sensors, microelectronics, data processors, and radars. Its surveillance and targeting system supported surface (the ATACMS) and air-launched, long-range conventional weapons delivering a mass of smart submunition (bomblets) that could break up massing follow-on echelons. The program led to developing an airborne moving target indication radar called the "Pave Mover." The system could detect, track, and target slow-moving armored vehicles allowing long-range surface and air missiles to launch attacks.[64]

The Soviets took notice of Assault Breaker when DARPA publicly demonstrated many of the required technological capabilities in 1976. In 1979, the Soviets simulated the Assault Breaker concept in a wargame. The game revealed

their European strategy was useless if Assault Breaker worked as advertised. By 1982, the United States had publicly demonstrated the Assault Breaker system; by 1983, some of the system's components were in production. In 1984, Marshal Ogarkov declared that the United States had achieved a "military-technical revolution" with its systems.[65]

Both the Soviets and Americans recognized that the switch from analog to digital technologies and the increasing use of space-based systems for reconnaissance and communication allowed for the necessary real-time command and control of cross-domain operations. The Soviets further recognized that their estimate of a 10–12-year rearmament cycle had now greatly compressed. The current Soviet economy and the lessening of access to advanced Western technology in the post-détente environment resulted in a lack of capacity to match the U.S. military rearmament.[66]

The Soviet military was concerned. The requirement for computers, machine-tool manufacturing, and microelectronics was essential to compete in the military-technical revolution. Yet, Soviet industry no longer sufficed, and the political support to fix the problem seemed limited. Marshal Ogarkov, wanting to keep pace with a growing Western military technology advantage, constantly argued for more money and improved military industry practices.[67] There was no money to be had. The Cold War landscape evolved, and a generational change occurred within the Soviet leadership. Ogarkov, mainly because he continued demanding that more money be poured into revamping Soviet conventional forces for a war no one wanted, was demoted in September 1984.[68]

Computer Arms Race Comes to a Head

What led to the rise in U.S.-Soviet tensions were the events of 1983. On 8 March, Reagan called the Soviets the "focus of evil in the modern world" and advocated for deploying the Pershing II and GLCM missiles (delivered in November 1983) to Europe.[69] Fifteen days later, he announced his support for developing a Strategic Defense Initiative (SDI) against ballistic missiles. Soviet-U.S. tension continued to increase. In September, Soviet air defense forces mistook Korean Airlines 007 for a U.S. military reconnaissance aircraft. They downed the aircraft, killing all on board. A month later, terrorists killed 241 U.S. Marines in Lebanon, and the U.S. invaded Grenada to prevent the presumed "Soviet-Cuban militarization of the Caribbean."[70] In November, U.S. and NATO exercise Able Archer 83 confused the Soviet air and missile commands. The confusion, false warnings of U.S. missile launches from the Soviet's orbital early-warning system, and the heightened tension almost resulted in war.[71]

SDI, Reagan touted, rendered ballistic missiles "impotent and obsolete."[72] Such a system undermined the current strategic deterrence system by reducing the concepts of mutually assured destruction, seemingly violating the 1972 Anti-Ballistic Missile (ABM) Treaty. Dubbed the "Star Wars" program, the SDI announcement's timing and television delivery was dramatic. A spectacular Ce-

cil B. DeMille-esk event by the former movie actor leveraged the technology narrative to the utmost. Reagan believed in the SDI, or at least the concept's power to force the Soviets to reevaluate the current competitive landscape. However, many in his administration and America's European allies did not believe in the system, its feasibility, nor its goal. Reagan, nonetheless, oversold SDI's capabilities with significant effect on the Soviets.[73]

The technology for a weaponized laser system, the foundation of SDI, was still in its infancy. Developing such a system and a space-based platform to place it on was technically feasible. But the cost to develop the system was so great that it could cripple the U.S. economy before it was operational. Despite Reagan announcing the program, the U.S. military technology sector quietly argued to abandon the effort.[74] Soviet science and technology communities, according to informant Farewell, felt the same about developing a space-based laser system. The Soviets had abandoned the development of a similar system years earlier.[75]

Here, the Soviet's take versus make approach to the computer arms race came home to roost. The CIA saw an opportunity to exploit the Soviet's industrial espionage reliance Farewell had revealed. The CIA allowed certain documents to be "taken" by KGB operatives. The documents and other measures deceived the KGB into believing the United States' laser program had solved the vast technical problems and was building a weaponized laser.[76]

The confident Soviet empire of the 1970s, which had gained 10 countries since the Communist victory in Vietnam, was fading.[77] The Soviets could ill afford to spend more on a theoretical ABM system. They already spent 10–15 percent of gross national product (GNP) on the military and another 3 percent on operating the Soviet empire.[78] The spending was a drag on an already shaky economic system. Worse, the spending was gaining them little. The war in Afghanistan was not going well, and the CIA was secretly helping the mujahideen to ensure it remained that way.

Andrew Busch provides a summary of Reagan's doctrine at this time. The use of SDI, economic sanctions, improved U.S. and NATO military doctrine and weapons, coercive diplomacy, and an ideological offensive created for the Soviets what Eduard Shevardnadze, the last Soviet minister of foreign affairs (1985 to 1990), described as a "Gordian knot. . . . No matter where we turned, we came up against the fact that we would achieve nothing without normalization of Soviet/American relations."[79]

Reagan's doctrine honed the West's computer exceptionalism narrative and thrust it deeply into the Soviet psyche. Reagan wanted to "lean on the Soviets until they go broke." Information operations and the leveraging Assault Breaker, among other successes, supported the coercive diplomacy narrative of the West's technological superiority. The information approach used a narrative of military lethality to mold perception, what Edward Luttwak called "armed suasion."[80] Other U.S. offset technologies, however, were not openly revealed. The United States' decision regarding what and when military technologies were re-

vealed, if at all, was part of the information campaign. It exploited Soviet weaknesses of over relying on economic espionage by creating a subtle undertow in the technology superiority narrative. "What technologies do we not know about?" sowed doubt and uncertainty in Soviet military planning.[81]

Conclusions

The Cold War evokes powerful memories and important lessons for the national security community. The case of the computer arms race provides an opportunity to consider the integration of the military with the economic and diplomatic levers in strategic competition. Like during the Cold War, today's world continues to shift inside the information environment. Creating Wimex, new reconnaissance-to-strike complexes, and smart weapons was critical to the Cold War technological revolution in military affairs. Today, the growth of the cyber domain and artificial intelligence (AI) creates another technology revolution.

But the world today is different than in the 1980s. The 1970s and 1980s science and technology explosion were fueled by the capitalist market-oriented economy that created power far greater than the Soviet's government-controlled system. China has learned from the Soviet's Cold War mistakes. They have central party control of the economy but embrace a form of capitalism that makes it more resilient. China continues to look for comparative advantage through taking instead of making technology. They produce many products but less unique intellectual capital. The West's willingness to cooperate, often to create a better bottom line on the ledger sheet, provides China access to legal and illegal mechanisms allowing them to take the technology. The West makes China's theft easier. Using embargoes to protect the science and technology sector, as seen in the Cold War, has limited effects. Bolstering the embargoes by improving security within the defense industry and academic community is essential.

Using a strong narrative that ties efforts across the national levers of power is essential. Reagan's effort in the 1980s is an example of integrated strategic competition campaigning, a concept being discussed in current U.S. military doctrine. The military's role in Reagan's campaign was to create and maintain the narrative of peace through strength. He increased the U.S. military in size, creating, at least in certain areas, symmetry and a quantitative balance of power with the Soviets. More importantly, Reagan leveraged asymmetry in computer technology as an offset strategy. He honed the narrative of U.S. technological exceptionalism and the lethality of computer-infused warfare. Then, he plunged it deep into the Soviet psyche, creating deterrence, coercion, and strategic paralysis.

The role of today's U.S. military is as it was in the late Cold War. Certainly, symmetry is required, and some increase in the U.S. force and the addition of allies must balance China's increases. Asymmetry, the offset strategy, is where the United States must focus. New U.S. and allies' competition concepts and doctrine must lay the foundation for the technology offset effort. Demonstrat-

ing ever-increasing lethality and battlefield competency should be a goal. Increasing military power is deterrence, forcing China to consider foreign policy restraint, as Reagan did with the Soviets in the Caribbean. Showing a willingness to use the military, or at least the weapons systems, as in the case of support to Ukraine, helps legitimize technology-driven lethality. But these actions must be coupled with diplomatic efforts that deter China and Russia while encouraging them to reverse harmful foreign and domestic policies.

Computer technology and the social changes it brought were too significant to deny the Soviet Union access completely. Competing and cooperating became, for the Soviets and Americans, a delicate yet often exhausting dance. In the U.S. and China dance, the latter seems to be leading, initiating the transitions and steps. As China already has, the United States and the West must accept that competition with some cooperation is a more effective way to remain free of conflict. Remaining free of conflict buys time. And time is needed for the West's integrated strategic competition campaign of deterrence, coercive diplomacy, and generational leadership and societal changes to take effect against China, as they did against the Soviet Union.

Endnotes

1. Leslie H. Gelb, "Who Won the Cold War?," *New York Times*, 20 August 1992, sec. A.
2. Three concept documents describe this new perspective of strategic competition for the *Joint Force in Strategic Competition*, Joint Doctrine (JD) Note 1-22 (Washington, DC: Joint Chiefs of Staff, 2023); *Competition Continuum*, JD Note 1-19 (Washington, DC: Joint Chiefs of Staff, 3 June 2019); and *Joint Concept for Integrated Campaigning* (Washington, DC: Joint Chiefs of Staff, 2018).
3. Ronald O'Rourke, *Great Power Competition: Implications for Defense—Issues for Congress* (Washington, DC: Congressional Research Service, 2022), 6, 26–30.
4. Yudhijit Bhattacharjee, "The Daring Ruse that Exposed China's Campaign to Steal American Secrets," *New York Times*, 7 March 2023.
5. Brendan Thomas-Noone, "What the Cold War Can Teach Washington about Chinese Tech Tensions," *Brookings* (blog), 12 January 2021.
6. David L. Boslaugh, *When Computers Went to Sea: The Story of the Naval Tactical Data System, NTDS—Engineering and Technology History* (Los Alamitos, CA: Wiley-IEEE Computer Society, 2003), chaps. 1–3 provide a detailed discussion of the almost two-decade development of NTDS. See also Norman Friedman, *Network-Centric Warfare: How Navies Learned to Fight Smarter through Three World Wars* (Annapolis, MD: Naval Institute Press, 2009), chap. 7.
7. The first five chapters provide a detailed discussion of the NTDS and SAGE associated computer systems programs during 20 years. Boslaugh, *When Computers Went to Sea.*
8. Benjamin Peters, "From Cybernetics to Cyber Networks: Norbert Wiener, the Soviet Internet, and the Cold War Dawn of Information Universalism" (PhD diss., Columbia University, 2010), 171; *A History of the ARPANET: The First Decade* (Arlington, VA: Bolt Beranek & Newman, 1981), II–2.
9. For more on Baran's view, see his published papers at "Paul Baran and the Origins of the Internet," Rand, accessed 5 May 2022.
10. Paul Baran, *On Distributed Communications: I. Introduction to Distributed Communications Networks* (Santa Monica, CA: Rand, 1964), secs. "Standard Message Blocks" and "Switching."
11. *A History of the ARPANET*, II–5.

12. Baran's ideas were not accepted at first. When British researcher Donald Watts Davies of the National Physical Laboratory (NPL) independently came to the same theory proposing a concept similar to Baran's in 1965, distributed communications became accepted. For a list of Baran's 1964 publications, see "Paul Baran and the Origins of the Internet"; and Peters, "From Cybernetics to Cyber Networks," 182. Harris points out the other elements that make the internet possible were developed by others including Leonard Kleinrock at UCLA. In a February 2000 email to Davies, Baran offered: "You and I share a common view of what packet switching is all about, since you and I independently came up with the same ingredients."
13. Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics* 38, no. 8 (April 1965): 4.
14. For a thorough discussion on how the Soviet system works against the development and use of computers in the society, see David A. Wellman, *A Chip in the Curtain: Computer Technology in the Soviet Union* (Washington, DC: National Defense University Press, 1989), chap. 3.
15. Slava Gerovitch, "How the Computer Got Its Revenge on the Soviet Union," Nautilus, 9 April 2015.
16. Norman Friedman, *The Fifty-Year War: Conflict and Strategy in the Cold War* (Annapolis, MD: Naval Institute Press, 2000), 189–92.
17. "We will bury you!" (Russian: «Мы вас похороним!») is a phrase used by Khrushchev while addressing Western ambassadors at a reception at the Polish embassy in Moscow on 18 November 1956. Friedman, *The Fifty-Year War*, 211–15.
18. The U.S. intelligence community was closely tracking the Soviet efforts to computerize economic planning and execution. *Intelligence Memorandum: The 1959 Soviet Budget* (Langley, VA: Central Intelligence Agency [CIA], 1959); and *Prospects for Computers in the Soviet Economy* (Langley, VA: CIA, 1967).
19. Peters, "From Cybernetics to Cyber Networks," 198.
20. Peters, "From Cybernetics to Cyber Networks," 254.
21. Peters, "From Cybernetics to Cyber Networks," 247–54.
22. Slava Gerovitch, "InterNyet: Why the Soviet Union Did Not Build a Nationwide Computer Network," *History and Technology* 24, no. 4 (December 2008): 338, https://doi.org/10.1080/07341510802044736.
23. *National Intelligence Estimate: Soviet Strategic Defenses* (Langley, VA: CIA, 1972), 1–5.
24. Kitov created the first cybernetic department in the Soviet military in 1952, implemented the first use of computers (the Strela), and theorized the air and missile defense network in his PhD dissertation. He was the military's cybernetics champion. Kitov's report meant for Khrushchev was called the "red book" for the color of its cover. Kitov reemerged in 1962 at the new Institute of Cybernetics in Kyiv. Peters, "From Cybernetics to Cyber Networks," 248–49.
25. Peters, "From Cybernetics to Cyber Networks," 255–57.
26. Wellman, *A Chip in the Curtain*, 96.
27. Wellman, *A Chip in the Curtain*, 103.
28. Aram Ter-Ghazaryan, "Computers in the USSR: A Story of Missed Opportunities," Russia Beyond, 24 September 2014; James Titus, "Soviet Computing: A Giant Awakens?," *Datamation,* 15 December 1971, 38–41; and Wellman, *A Chip in the Curtain*, 71–75.
29. Many of the defectors discussed were tasked with economic espionage. Kevin P. Riehle, "Insider Information: The Strategic Windfall Gained from Soviet Intelligence Officer Defectors" (diss., King's College London, 2018). The case of Iosif Volodarsky and Gaik Ovakimyan conducting science and technology intelligence in the United States in 1935 is illustrative. Kevin P. Riehle, *Russian Intelligence: A Case-Based Study of Russian Services and Missions Past and Present* (Bethesda, MD: National Intelligence Press, 2022), 137.
30. Eugene S. Poteat, "The Attack on America's Intellectual Property Espionage after the Cold War," *Bent of Tau Beta PI* (Winter 2001): 14.
31. "Cold War Sanctions—Embargoes and Sanctions," American Foreign Relations, ac-

cessed 5 July 2022; and Adam Kline and Tim Hwang, *From Cold War Sanctions to Weaponized Interdependence* (Washington, DC: Center for Security and Emerging Technology, 2021), 3.

32. Frank Cain, "Computers and the Cold War: United States Restrictions on the Export of Computers to the Soviet Union and Communist China," *Journal of Contemporary History* 40, no. 1 (January 2005): 138, https://doi.org/10.1177/0022009405049270.
33. Cain, "Computers and the Cold War," 133–37; *COCOM Countries' Sales of Technology to the USSR and Eastern Europe* (Langley, VA: CIA, 1970), 1–3.
34. Mario Daniels, "Safeguarding Détente: U.S. High Performance Computer Exports to the Soviet Union," *Diplomatic History* 46, no. 4 (September 2022): 8, https://doi.org/10.1093/dh/dhac031. For details, see "U.S. Policy on the Export of Computers to Communist Countries," National Security Department Memo 247.
35. Daniels, "Safeguarding Détente," 4–9.
36. Before 1967, no requests for CoCom exemption had been submitted. After the relaxation of controls by the 1967–69 CoCom List Review, 32 requests for exemption were submitted in the first 7 months of 1970. See "COCOM Countries' Sales of Technology to the USSR and Eastern Europe."
37. Rein Turn, *U.S. vs IBM: The Computer Gap and National Security: Implications for Relaxing Export Controls*, Working Note (Santa Monica, CA: Rand, 1973).
38. "The Soviet computer industry is a troubled and lagging sector of the Soviet economy." "Production of Computers in the USSR," Intelligence Memorandum, CIA, July 1971, 1.
39. The "gap" theory can also be part of a general civilian-military perception and communication problem. Thomas S. Szayna et al., *The Civil-Military Gap in the United States: Does It Exist, Why, and Does It Matter?* (Santa Monica, CA: Rand, 2007). For more discussion on bomber and missile gaps, see John Prados, *The Soviet Estimate: U.S. Intelligence Analysis & Russian Military Strength* (New York: Dial Press, 1982), chaps. 4 and 8. For a discussion regarding the concept of the offensive/defensive balance of military technology, see Jack S. Levy, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis," *International Studies Quarterly* 28, no. 2 (1984): 219–38, https://doi.org/10.2307/2600696.
40. "Nixon Seeks Sweeping New Power," *New York Times*, 15 April 1973, sec. Archives.
41. For more on the assessed benefits to the Soviets from détente, see *Soviet Economic and Technological Benefits from Detente* (Washington, DC: CIA, 1974); An Act to Promote the Development of an Open, Nondiscriminatory, and Fair World Economic System, to Stimulate Fair and Free Competition Between the United States and Foreign Nations, to Foster and Economic Growth of, and Full Employment in, The United States, and for Other Purposes. H.R. 10710, 93d Cong. (1973).
42. *An Analysis of Export Controls of U.S. Technology—A DoD Perspective* (Washington, DC: Office of the Director of Defense Research and Engineering, 1976), 25.
43. "A Short History of NATO," NATO, accessed 27 March 2023; and "The Euromissile Showdown," *Air & Space Forces Magazine* (blog), accessed 30 March 2023.
44. John Lewis Gaddis, *Strategies of Containment: A Critical Appraisal of American National Security Policy During the Cold War* (Cary, NC: Oxford University Press, 2005), 342–49; and Jeremy Kuzmarov, "The Improbable Militarist: Jimmy Carter, the Revolution in Military Affairs and Limits of the American Two-Party System," *Class, Race and Corporate Power* 6, no. 2 (2018): https://doi.org/10.25148/CRCP.6.2.008311.
45. *NSDD 75 on "U.S. Relations with the USSR"* (Washington, DC: White House, 1983).
46. Gaddis, *Strategies of Containment*, 356–57.
47. Leslie H. Gelb, "Reagan's Military Budget Puts Emphasis on a Buildup of U.S. Global Power," *New York Times*, 7 February 1982.
48. *NSDD 75 on "U.S. Relations with the USSR,"* 7.
49. Andrew E. Busch, "Ronald Reagan and the Defeat of the Soviet Empire," *Presidential Studies Quarterly* 27, no. 3 (1997): 454. See also Gaddis, *Strategies of Containment*,

chap. 11. Regarding the policy and the role of the U.S. military, see *NSDD 75 on "U.S. Relations with the USSR,"* 7.

50. Gaddis, *Strategies of Containment*, 348.
51. Bruce W. Jentleson, "The Reagan Administration and Coercive Diplomacy: Restraining More than Remaking Governments," *Political Science Quarterly* 106, no. 1 (1991): 58–59, https://doi.org/10.2307/2152174. Reagan's idea to use limited force while displaying the ability to deliver far more conventional force destruction came partly from a 1975 study by Barry Blechman and Stephen Kaplan. Blechman and Kaplan showed that direct military action attains desired outcomes for only a short period. Barry M. Blechman and Stephen S. Kaplan, *Force without War: U.S. Armed Forces as a Political Instrument* (Washington, DC: Brookings Institution, 1978).
52. Jentleson, "The Reagan Administration and Coercive Diplomacy," 58–59; and Blechman and Kaplan, *Force without War.*
53. *NSDD 75 on "U.S. Relations with the USSR,"* 3–4.
54. A nine-volume study. Barry W. Boehm and Allen C. Haile, *Information Processing/Data Automation Implications of Air Force Command and Control Requirements in the 1980s,* vol. 11, *Roadmaps* (Los Angeles, CA: Space and Missile Systems Organization, 1972). Ware discusses the other Rand studies. Willis H. Ware, *Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security* (Santa Monica, CA: Rand, 1979), https://doi.org/10.7249/R609-1.
55. Sergei Kostin et al., *Farewell: The Greatest Spy Story of the Twentieth Century* (Las Vegas, NV: AmazonCrossing, 2011). See also Christopher M. Andrew and Oleg Gordievsky, *KGB: The Inside Story of Its Foreign Operations from Lenin to Gorbachev*, 1st ed. (New York: HarperCollins, 1990), 623.
56. Prime provided the Soviets with an estimated $1 billion of signals intelligence during 22 years. Walker provided the KGB with U.S. Navy communication equipment technical details and encryption key codes for 17 years. Andrew and Gordievsky, *KGB,* 524–31.
57. Congress investigated and eventually passed the Computer Security Act in 1987. Michael Warner, "Cybersecurity: A Pre-History," *Intelligence and National Security* 27, no. 5 (2012): 786–88, https://doi.org/10.1080/02684527.2012.708530.
58. For a deeper discussion on doctrine and its role, see Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: U.S. Naval War College, 2009), chap. 12.
59. NATO retained Flexible Response as its primary doctrine. AirLand Battle and the subconcept of Follow-on Forces Attack (FOFA) forced NATO to discuss the implications of emerging military technologies. Douglas W. Skinner, *AirLand Battle Doctrine* (Arlington, VA: CNA, 1988), 1. A discussion regarding the need to consider resource planning for the concepts of AirLand Battle and its subconcepts is discussed. *Proceedings of the Third International Seminar: The Current Debate on NATO Strategy* (Rome, IT: Research Division, NATO Defense College, 1985), 64–67; *Long Term Planning Guideline for Follow-on Forces Attack was approved by NATO in 1984. Michael J. Diver, NATO's Follow-On Forces Attack (FOFA) Concept: Past, Present and Future* (Fort Belvoir, VA: Defense Technical Information Center, 1990), https://doi.org/10.21236/ADA224090.
60. Diego A. Ruiz-Palmer, *Theatre Operations, High Commands and Large-Scale Exercises in Soviet and Russian Military Practice Insights and Implications* (Rome: Research Division, NATO Defense College, 2018).
61. Skinner, *AirLand Battle Doctrine*, 6.
62. Skinner, *AirLand Battle Doctrine*, 25.
63. R. Kent Laughbaum, *Synchronizing Airpower and Firepower in the Deep Battle* (Maxwell AFB, AL: Air University Press, 1999).
64. Skinner, *AirLand Battle Doctrine*, 25; Pave Mover was redesignated as Joint Surveillance and Target Acquisition System (JSTARS) in the 1980s. "JSTARS," DARPA, accessed 31 March 2023.
65. Octavian Manea, "The Role of Offset Strategies in Restoring Conventional Deter-

rence," interview with Robert O. Work, the 31st Deputy Secretary of Defense, *Small Wars Journal*, 4 January 2018.

66. Notra Trulock III, Kerry L. Hines, and Anne D. Herr, *Soviet Military Thought in Transition: Implications for the Long-Term Military Competition*, PSR Report No. 1831 (Arlington, VA: Pacific-Sierra Research, 1988), 42–53.
67. Trulock, Hines, and Herr, *Soviet Military Thought in Transition*, 54–58; and Gordon S. Barrass, "The Renaissance in American Strategy and the Ending of the Great Cold War," *Military Review*, February 2010.
68. Barrass, "The Renaissance in American Strategy and the Ending of the Great Cold War."
69. Ronald Reagan, "Ronald Reagan, 'Evil Empire Speech'," *Voices of Democracy* (blog), 8 March 1983.
70. Not everyone agreed with the United States. The United Nations General Assembly adopted a resolution on 2 November 1983 "deeply deploring" the invasion of Grenada as "a flagrant violation of international law." Grenada's nearest neighbors and Israel voted with the United States against the resolution, which passed by a vote of 108 to 9. John T. Correll, "The Grenada Adventure," *Air & Space Forces Magazine*, 1 November 2012, 64.
71. Declassified documents revealed that U.S. intelligence recognized that the Soviets had increased their alert posture and war footing. Cooler heads in the lower levels of operational C2 prevented an escalation. See declassified documents: "Able Archer War Scare 'Potentially Disastrous'," National Security Archive, accessed 31 March 2023; and "Able Archer 83 Nearly Sparked Nuclear War with the Soviets," *Smithsonian Magazine*, 27 April 2022.
72. "Strategic Defense Initiative (SDI)," Atomic Heritage Foundation, 18 July 2018.
73. "Strategic Defense Initiative (SDI)." Regarding SDI's part in undermining Soviet strategy. Busch, "Ronald Reagan and the Defeat of the Soviet Empire," 455–60.
74. "Strategic Defense Initiative (SDI)."
75. Kostin et al., *Farewell*, 284–86.
76. Kostin et al., *Farewell*, 284–86.
77. Busch, "Ronald Reagan and the Defeat of the Soviet Empire," 451.
78. The CIA estimated 15–17 percent and a 1980 Rand study on the Soviet Empire offered as much as 21.4 percent in 1980. Holzman argues the numbers are inflated and should be 8–10 percent of Soviet GNP. Franklyn D. Holzman, "Politics and Guesswork: CIA and DIA Estimates of Soviet Military Spending," *International Security* 14, no. 2 (1989): 101–31, https://doi.org/10.2307/2538856. The empire is described as those Soviet Bloc states and periphery states they wished to influence. Charles Wolf Jr. et al., *The Cost of the Soviet Empire* (Santa Monica, CA: Rand, 1983), https://doi.org/10.7249/R3073.1.
79. Busch, "Ronald Reagan and the Defeat of the Soviet Empire," 461–62.
80. Edward Luttwak, *The Political Uses of Sea Power* (Baltimore, MD: Johns Hopkins University Press, 1974); and James R. Holmes, "You Have to Be There," U.S. Naval Institute *Proceedings* 148, no. 7 (July 2022).
81. Robert Tomes, "Why the Cold War Offset Strategy Was All about Deterrence and Stealth," *War on the Rocks*, 14 January 2015.