SYM-AM-22-092

Excerpt from the Proceedings of the Nineteenth Annual Acquisition Research Symposium

Acquisition Research: Creating Synergy for Informed Change

May 11–12, 2022

Published: May 2, 2022

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

The research presented in this report was supported by the Acquisition Research Program at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact any of the staff listed on the Acquisition Research Program website (www.acquisitionresearch.net).

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School

Acquisition Warfare: A Proposal for a Unifying Concept

Lieutenant Commander Ryan Hilger—is an active duty Navy Engineering Duty Officer who served onboard USS Maine (SSBN 741; GOLD), as Chief Engineer of USS Springfield (SSN 761), and ashore with the CNO Strategic Studies Group XXXIII, at OPNAV N97, and on tours as an Engineering Duty Officer. He holds a BA in political science from the University of Kansas, an MS in mechanical engineering from the Naval Postgraduate School, and is a doctoral student in systems engineering at Colorado State University. His opinions are his own and do not reflect the official position of the Department of Defense. [rphilger@colostate.edu]

Abstract

The ongoing debate in the United States over defense acquisition reform highlights the complexity and evolution of the national security ecosystem. That complexity, explored using a first order system dynamic model, indicates that defense acquisition reform may be a so-called "super wicked" problem. Solutions to super wicked problems form a new class of solutions than traditionally found in the literature for defense acquisition reform. This paper asserts that defense acquisition reform is a super wicked problem and that adoption of an ecosystem model from the program office's perspective will yield new insights into ecosystem dynamics. Additionally, American adversaries, principally China and Russia, have used a variety of tactics and operations in systemic campaigns targeting the liminal space within the defense acquisition ecosystem. This paper proposes the unifying concept of acquisition warfare to better describe the set of adversary actions and how they disrupt the ability of program managers to successfully deliver their programs, not just systems, uncompromised within cost, schedule, and performance constraints.

Introduction

Over the last 70 years, the Department of Defense (DoD) acquisition system has continually evolved to meet perceived changes in the international threat environment, priorities from Congress of a new presidential administration, or the whims and preferences of key leaders. Researchers at the Center for Strategic and International Studies observed that within those 70 years, the DoD has initiated eight different acquisition reform cycles, split evenly between centralizing and decentralizing reforms (Dwyer et al., 2020). Today, the American defense establishment is again gripped by great power competition, simultaneously calling for faster action to retain American supremacy on the battlefield while bemoaning the lack of progress in acquiring weapons systems faster. The ebb and flow of changes mimics the patterns found in life, not the static, monolithic structure that we perceive the DoD to be.

The nature of these reforms and the cyclical patterns indicate that, despite professed desires, the national security establishment has not yet gotten defense acquisition reform "right." That psychological dissatisfaction with the status quo finds firmer theoretical grounding when viewed as a wicked problem, a term first coined by Horst Rittel and Melvin Webber in 1973 (Rittel & Webber, 1973). Levin et al. (2012) introduced a variation of wicked problems that especially fit the lingering discontent: super wicked problems. The particularly nasty planning problems exhibit additional characteristics that fit well with defense acquisition reform: urgency, lack of a single responsible entity to solve it, and humans acting as humans are wont to do—irrationally. As the problem evolves, so must the solution space, which means that we never solve the same problem twice.

To bring cohesion to the problem of defense acquisition reform and unify that problem with the latest round of international pressure, this paper offers two hypotheses. First, defense acquisition reform is a super wicked problem based on the behaviors and structure of the defense ecosystem. Second, a new theory of acquisition warfare represents a novel approach to understanding both the frustrations with reform and the avenues by which adversaries exploit

the features of the ecosystem for their relative advantage. To support both hypotheses, this paper also develops a first attempt at a model of the defense ecosystem from the particular perspective of a defense acquisition program office.

Defense Acquisition Reform as a Super Wicked Problem

In their seminal 1973 paper on "Dilemmas in a General Theory of Planning," Horst Rittel and Melvin Webber defined a new class of planning problems as wicked problems, including an explicit mention of the new Planning, Programming, and Budgeting System developed under Secretary of Defense Robert McNamara (Rittel & Webber, 1973). At its core, the Defense Acquisition System (DAS), comprised of the Planning, Programming, Budgeting, and Execution (PPBE) system, the Joint Capabilities Integration and Development System (JCIDS), and the acquisition system, is a planning system. In its idealized form, planning is about explicit definition of a problem, articulation of desired goals or outputs, and the alignment of the fewest resources needed to accomplish the goal. In the DAS, executing the process of delivering a capability or system from start to finish is an idealized process that all in the defense acquisition and requirements space are familiar with. Rittel and Webber (1973), however, cast doubt on the efficacy of such systems: "And yet we know that such a planning system is unattainable, even as we seek more closely to approximate it. It is even questionable whether such a planning system is desirable." Indeed, those words remain equally true in 2022 as they were in 1973 as Congress launches a new commission to reform the PPBE process (Lineweaver et al., 2013; Serbu, 2021).

For these large scale planning, or wicked, problems, Rittel and Webber (1973) distilled 10 identifying characteristics: 1) no definitive formulation of the problem; 2) the problem does not stop, it just changes; 3) solutions are relatively good or bad; 4) there is no immediate test for efficacy of solutions; 5) every attempt at a solution is a "one-shot" operation since it changes the system; 6) the number of potential solutions are innumerable; 7) each problem is unique; 8) each wicked problem can be considered a symptom of another problem; 9) discrepancies have no single defining explanation; and 10) the planner has no right to be wrong (Rittel & Webber, 1973). In 2012, Levin et al. expanded Rittel and Webber's conceptualization of the wicked problem to encompass particular governance or policy planning problems where human behavior is irrationally biased toward short-term time horizons despite the more severe long-term impacts of those actions. These "super wicked" problems have four additional primary characteristics in addition to the original 10: "time is running out; those who cause the problem also seek to provide a solution; the central authority needed to address them is weak or non-existent; and irrational discounting occurs that pushes responses into the future" (Levin et al., 2012).

While Rittel and Webber (1973) originally characterized the Defense Acquisition System as a wicked problem, it fits better under the super wicked problem framework proposed by Levin et al. (2012). J. Ronald Fox et al.'s (2011) analysis in "Defense Acquisition Reform 1960-2009: An Elusive Goal" shows the overwhelming need for coordination amongst all stakeholders within the defense acquisition ecosystem, which reflects the lack of a centralized governance structure and the reaction to changes in the environment—mostly the Soviet Union—and the difficulty of producing an enduring solution (Fox et al., 2011).

Today, many of those same leaders still work within the defense acquisition ecosystem, and again the national security establishment espouses a driving need to reform the system in response to renewed global competition from a resurgent Russia and a rapidly growing China. The DoD's annual report to Congress for 2021, required by Congress since 2000, reports that the People's Republic of China has set a near-term military modernization goal of 2027 to provide additional, credible options for use against Taiwan as part of their longer-term goal of

achieving a dominant military position by 2049 (*Military and Security Developments Involving the People's Republic of China*, 2021). The report certainly has a bias to it given the incentive for the DoD to inflate risks and consequences in an effort to secure additional funding from Congress, but the general content of the report can be independently confirmed by independent analysts on China and other open-source reporting. As a result, over the last few years, DoD officials, as summarized by the Congressional Research Service in their "Report to Congress on Great Power Competition," continue to stress that the time available to modernize the military is running out—China will surpass American military capabilities without significant investment and reform of all aspects of the defense ecosystem (*Renewed Great Power Competition: Implications for Defense-Issues for Congress*, 2022).

News articles from a one-week period in May 2021 alone highlight how different stakeholders have different perspectives on the issue, and example headlines range from "We Are Lost in the Woods on Defense Acquisition Reform" to "Acquisition Reform Is Making Rapid Progress, Defense Official Says" to "Just in: Pentagon 'Doubling Down' on Acquisition Reform" (Tadjdeh, 2021; Vergun, 2021; Welter, 2021). Other efforts from Congress over the last few years have required the DoD to examine reforms to the acquisition system writ large with the Section 809 panel, to smaller reform efforts for software acquisition practices, contracting options, and more (*Advisory Panel on Streamlining and Codifying Acquisition Regulations Volume 3 of 3 Summary of Recommendations*, 2019). The former Under Secretary of Defense for Acquisition and Sustainment, Ellen Lord, even enacted the most sweeping changes to Defense Systems Engineering in decades with the complete overhaul and reissuance of Department of Defense Directive 5000.01, taking the DoD from a traditional waterfall-centric systems engineering model to a "choose your own adventure" set of pathways for programs to choose from in an effort to streamline and accelerate acquisition of defense systems (*DoDD 5000.01 The Defense Acquisition System*, 2020).

Despite the clarion call to action for more aggressive reforms with respect to Chinese modernization, little progress seems to be made beyond small efforts with localized, and often temporal, results. Defense officials, Congress, presidential administrations, and the acquisition workforce all understand the pressing need to accelerate their efforts and deliver capability and capacity more rapidly, but the data shows that existing programs are continuing to execute their plans and Defense leaders have made little headway with Congress in divesting of legacy programs in favor of new technologies, changing acquisition strategies and pathways for major defense programs, and continue to have problems in meeting cost, schedule, and performance objectives ("High Risk Area - DOD Weapon Systems Acquisition," n.d.). In some cases, the DoD appears to be moving opposite from the direction of reform by slipping new programs further in the future, continuing to buy legacy systems as a result of delays to new programs, and sinking additional costs into these legacy programs from organizational inertia to modernize them to the limits of their available margins—the Concorde effect or sunk cost fallacy on a large scale (Arkes & Ayton, 1999). DoD weapon system acquisition first made the Government Accountability Office's (GAO's) High Risk list in 1990, providing a detailed longitudinal view of defense acquisition, but the GAO reports that despite strong leadership commitment in the last few years, progress remains significantly hindered ("High Risk Area - DOD Weapon Systems Acquisition," n.d.). Thus, despite strong Congressional support, committed DoD acquisition leadership and workforce, and a pressing, time-driven need, little change is occurring in the ecosystem—truly a super wicked problem. Perhaps a new approach to understanding the defense acquisition system is needed. Combining the disparate elements into a broader ecosystem model may yield new insights into how the defense acquisition ecosystem functions and reveal potential solution paths that could alter ecosystem behaviors and dynamics.

The Program Ecosystem

An ecosystem is a complex and coherent system of biophysical and social factors capable of adaptation and sustainability over time. While ecosystems generally conjure images of nature, the underlying principles govern human ecosystems as well. Ecosystems have structure which may or may not be directly observable (Margalef, 1963). The ecosystem may be observed indirectly through various metrics, behaviors, and trends within the ecosystem. In the case of defense acquisition, this includes measurable properties such as federal funding, employees, counts of weapons systems, etc., even though those metrics do not directly measure the structure and rules of the ecosystem. That structure, according to Ramon Margalef (1963), becomes "more complex, more rich, as time passes; structure is linked to history." The richness and evolution of the defense acquisition system, as chronicled by J. Ronald Fox et al. (2011), proves that, even though the system still seeks to produce the same outputs, the way in which it structures itself and alters the resource and information flows adapts and changes over time in response to various changes. Burch et al. (2017) developed the Human Ecosystem Model, shown in Figure 1, to better show general ecosystem dynamics and behaviors. Given that ecosystems are dynamic systems, the actors cannot produce observable behaviors or the measurable metrics without some exchange or flow of resources. Burch et al. (2017) identify six flows in the Human Ecosystem Model: individuals, energy, nutrients, materials, information, and capital (Burch et al., 2017). Other than nutrients, perhaps, all of these are applicable to driving action for producing decisions, capabilities, and outcomes in the defense acquisition system.

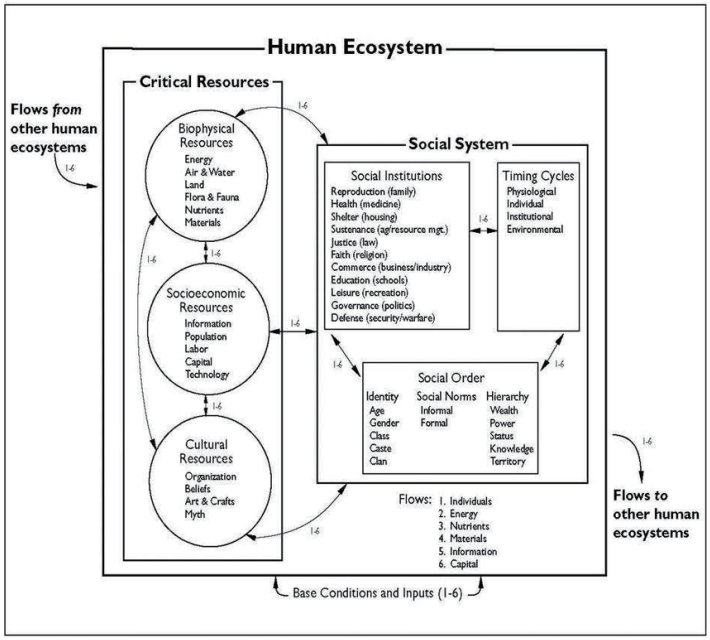

Figure 1. Human Ecosystem Model Developed by Burch, Machlis, and Force (2017)

In this context, *the program ecosystem is the coherent collection of people, processes, and systems working in the surrounding physical, cyber, and information domains to design, develop, produce, operate, and sustain national security systems and is viewed from the perspective of a defense acquisition program office*. That ecosystem can be modeled to show the dynamics that influence the behavior within that ecosystem. Figure 2, below, presents a simplified model of a defense program ecosystem. The simplified and local detailed models were developed primarily from the author's personal experience and required professional development activities as a generic, normative model of a defense acquisition program office, and do not necessarily represent the ecosystem of a specific program within the DoD.

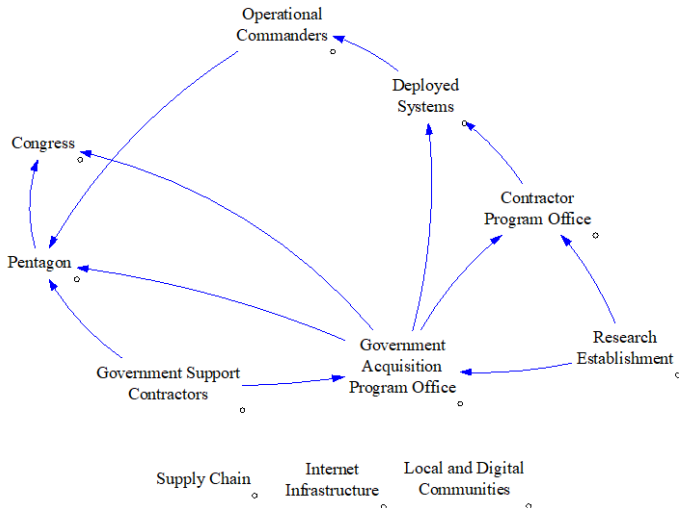

Figure 2. Simplified Program Ecosystem Model

The model reveals that a defense acquisition program does not operate in a vacuum, but rather within the broader environment, which in turn is impacted on the larger forces acting on the national security-industrial base, global supply chains, and the national and international environments. In turn, the entire ecosystem is supported by the physical and digital communities the workforces are a part of, the supply chains that provide individuals with their basic needs and the program with its material, and the internet that underpins the fabric of modern society. Thus, the program ecosystem is a complex adaptive system that exhibits emergent behaviors as the forces and flows of the ecosystem change over time. At the level of the program manager, the ability to control the cost, schedule, and performance of their given program is subject to the complexity of the ecosystem and the forces acting on the ecosystem at all levels, not just the deployed weapon system. Developing and generating effective combat power requires the flow of resources through the program ecosystem, notionally starting with requirements validation in the Pentagon, Congressional authorization and appropriation of funding, and expenditure of funds to design, develop, deploy, and sustain these systems. People at every node in the ecosystem have their own processes and procedures to execute to complete their step in the system value stream.

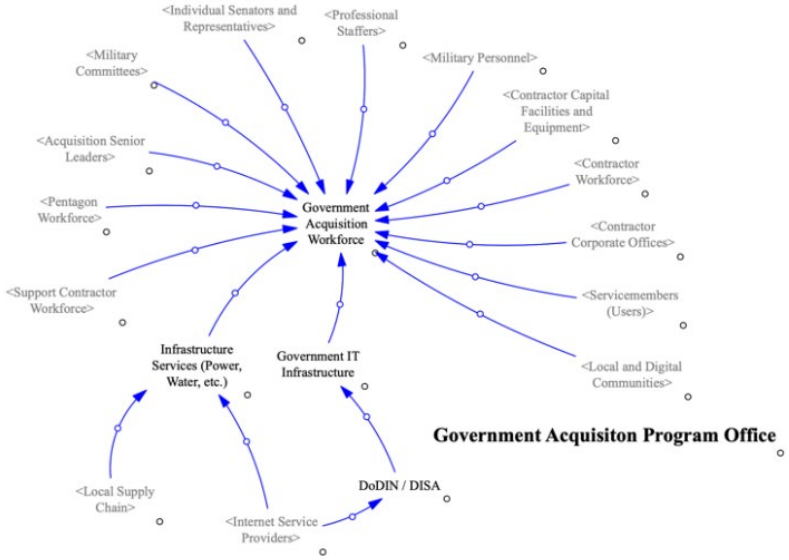

Figure 3. Detailed System Model of a Government Acquisition Program Office

The major actors in the ecosystem, the workforce of various organizations, do the daily work of defending the nation from conceiving of initial capabilities to designing and producing systems to conducting deployed operations. The relationships show how each of those major actors interact within the ecosystem. As the model shows, each of these people goes about their business dependent on the whole ecosystem. People have homes, are part of their local communities, are reliant on local infrastructure services and supply chains, and have digital lives depending on their local internet service providers. Thus, the forces acting on each of the people in a defense acquisition program ecosystem influence their daily behavior and their ability to focus on the program. Combined with the underlying infrastructure that supports human activity, the program ecosystem also represents a system view of a program's attack surface and the various propagation paths for vulnerabilities or other adversarial effects to disrupt the program or its deployed system. To provide better insight into how the ecosystem works, we provide a detailed model of several of the major actors and a brief description of the behaviors observed.

Government Program Office

Figure 3 shows the web of relationships that employees in a defense acquisition program must manage daily and the resources that go into supporting their daily work. Each day may find the program manager defending their program before Congress, meeting with leaders in the Pentagon to determine future years budget strategies and giving program updates, meeting with industry suppliers and their contractors, liaising with the servicemembers using their systems, and planning and scheduling modernization and deployment efforts with their commanders.

Contractor Program Office

Figure 4 shows the contractor's program office is equally complex, though the detailed model shows a different network of relationships that they must maintain and different forces that influence contractor behavior. As the contractor works the systems engineering lifecycle, they interact with suppliers at many levels, the government entities, including Congress through lobbying organizations, and the deployed systems, inclusive of the hardware, software, and users, to sustain the system.

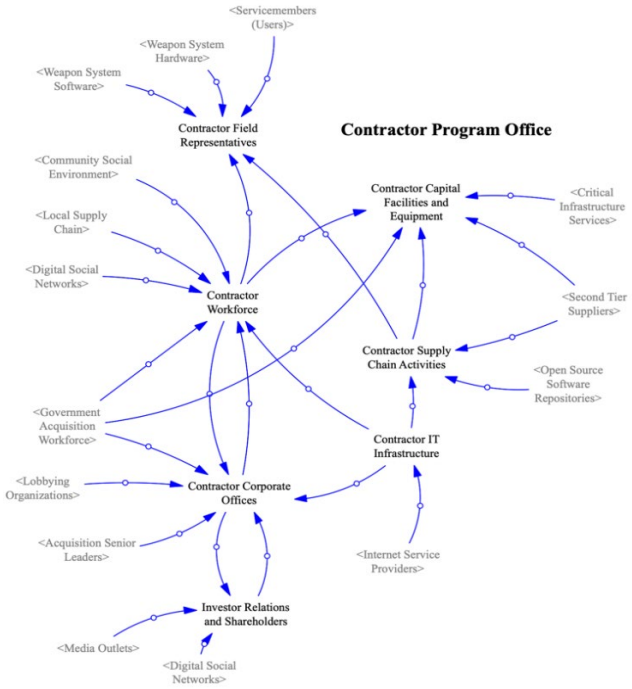

Figure 4. Detailed Model of a Contractor Program Office

Pentagon

The Pentagon, the long-standing nexus of defense acquisition funding and top-level requirements, operates in an equally complex web within the program ecosystem, as shown in Figure 5. Focusing specifically on the acquisition role in the Pentagon, the acquisition workforce and senior leaders work closely with Congress, the defense program offices, the business development offices of defense contractors, the media, and the military commanders to ensure that the defense program office has the resources to meet the requirements requested by those military commanders.

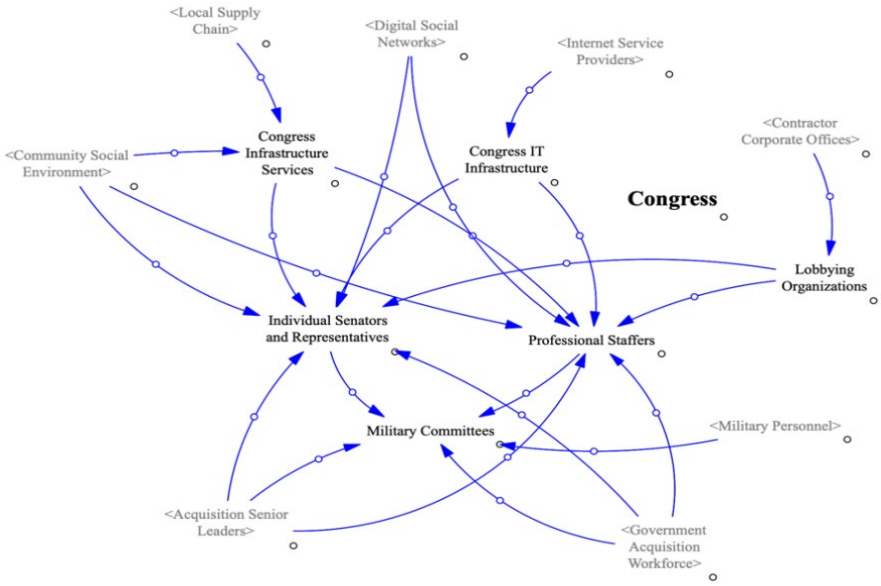

Figure 5. Detailed Model of the Pentagon Ecosystem

Congress

Congress retains the constitutional authority to authorize program, appropriate funds, and set broad policy guidance through changes to federal law. As the model shows, both the individual Senators and Representatives and their professional staffs craft the laws. Those laws authorize defense programs to exist and appropriate funds for the program to execute. This process is influenced by several external entities. The external entities come from the local community in Washington D.C., where most of the Congressional workforce resides, as well as from the acquisition workforce in the program offices and the Pentagon, and from various lobbying organizations for the defense industrial base.

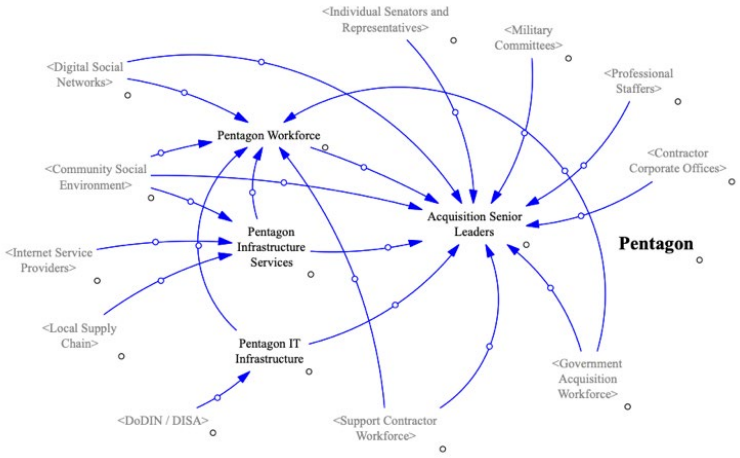

Figure 6. Detailed Model of the Congressional-Military Ecosystem

Deployed Weapon System

As shown in Figure 7, the deployed system is a scalable concept that ranges from an individual piece of equipment to a warship, satellite constellation, or long-range missile—anything produced through the Defense Acquisition System. In the program ecosystem, the deployed system can be defined as the hardware, software, the users of the system, and how they interact with the broader military environment. The servicemembers are influenced by the local community and its ability to sustain a population, their digital communities, and how they interact with the contractor's field representatives and the government program office to operate and sustain their systems.

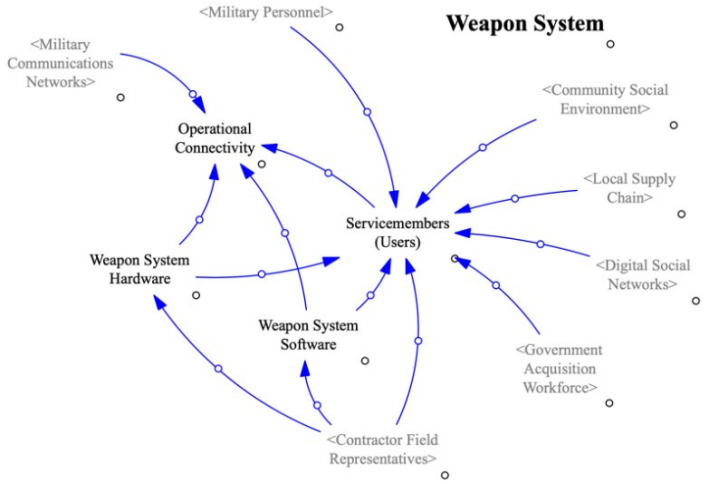

Figure 7. Detailed Model of a Deployed Weapon System

Research Ecosystem

The research ecosystem, modeled in Figure 8, represents the initial conception and early development of future capabilities. There are various actors, ranging from academia for basic research to mature research and development organizations for more complex prototypes and proofs of concept. Each of these organizational types have different incentives and influences to support and drive their research agendas. Like the other subcommunities within the program ecosystem, the researchers and their organizations are supported and influenced by their physical and digital communities.

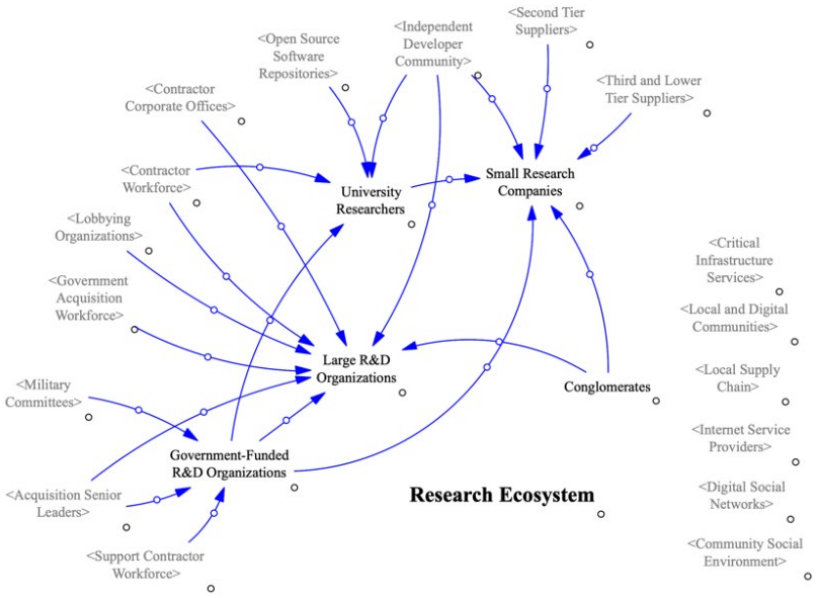

Figure 8. Detailed Model of the Defense Research Ecosystem

Local Community

Though often forgotten in the defense acquisition process, the local communities where the various program activities take place play a significant role in shaping individual and organizational behavior. The local community, shown in Figure 9, comprises two major parts: physical and digital. The physical communities are the neighborhoods and cities where people physically live, the civic and social activities we undertake during our lives, and the supply chains that provide for the basic needs and wants of the community. The digital communities, which include media outlets, have taken a major role in our lives and play an increasingly significant role in shaping our behaviors and attitudes, which spill into our work environment and shape the growing trend of digital nomadism (Reichenberger, 2017).

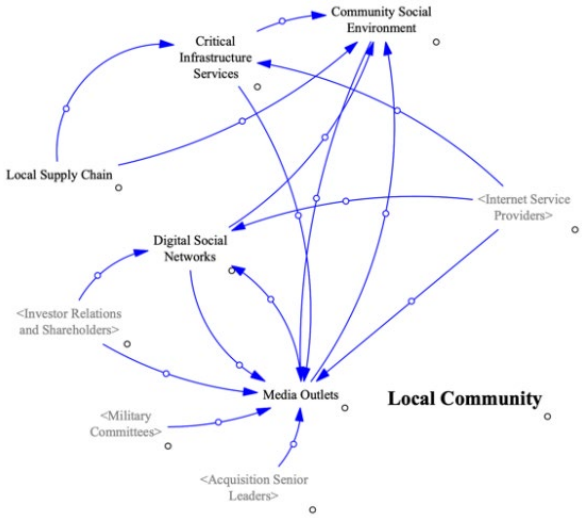

Figure 9. Detailed Model of the Local Community as It Supports the Program Ecosystem

In considering the hypothesis of defense acquisition reform as a super wicked problem, the complexities of the issues come through when viewed through the lens of the program ecosystem. Many recent reform proposals target aspects of the program ecosystem, but in light of the relationships between the entities, it shows how difficult implementing effective change can be. For example, the Section 809 Panel, chartered by the Fiscal Year 2016 National Defense Authorization Act, conducted a comprehensive study and produced 93 different recommendations for streamlining defense acquisition (*Advisory Panel on Streamlining and Codifying Acquisition Regulations Volume 3 of 3 Summary of Recommendations*, 2019). These recommendations primarily support the defense program office in the ecosystem model and do not consider the proposals and needs for reform of Congressional processes, JCIDS processes and requirements management in the Pentagon, improving the defense industrial base, etc., nor the previous recommendations of Congressionally chartered studies, the defense advisory boards, or industry studies.

The sheer volume of recommendations from the myriad studies is symptomatic of a deeper concern within the functioning of the program ecosystem. Rapport et al. (1985) state that the "signs or symptoms of distressed ecosystems do not generally appear in isolation" and that there are key indicators of overall ecosystem health that can be monitored. The authors cite several studies showing "reductions in species diversity, increases in nutrient leaching," the "simplification of the structure of plant and animal communities … and loss of part or all of the inventory of nutrients," or the "shift away from complex arrangements of specialized species toward the generalist … away from diversity in birds, plants and fish toward monotony" (Rapport et al., 1985). In the program ecosystem, we see the steady consolidation of the defense industrial base to a smaller number of large defense contractors (reduction in species diversity and simplification of the structure akin to the transition from polyculture to monocropping in agriculture) and an increasing share of defense dollars going toward those consolidated defense contractors (nutrient leaching or loss of nutrients; Berenson, 2021; *Department of Defense Report State of Competition within the Defense Industrial Base*, 2022; Jang et al., 2021). Rapport at al. (1985) continue, stating "there is an evident linkage among features of a distressed ecosystem… changes in primary productivity are linked with changes in nutrient availability" and that the symptoms of an ecosystem in distress can only be viewed in retrospect, akin to vital signs in medicine that indicate a disease has already advanced (Rapport et al., 1985). Adversaries seeking to slow the ability of the DoD to credibly and reliably develop and generate global combat power will necessarily target the program ecosystem at its weakest

points or at the points where action may result in the greatest leverage or compounded effects. The concept of acquisition warfare provides a novel and analogous approach to address the complexity present in the ecosystem as recent approaches to climate change and global health have with the “One Health” and “One Medicine” initiatives that have undertaken to unify the disparate elements and theories within the ecosystem (Zinsstag et al., 2011).

Acquisition Warfare

The United States’ adversaries operate with the same forces in the global environment and recently have proven more adept at leveraging non-kinetic means at the liminal edge of conflict. Liminality represents the zone between detection and overt response and has rapidly grown to be the prime maneuver space for adversaries seeking to engage the United States at levels below those that would trigger escalatory actions, such as use of force, economic sanctions, etc. The United States, on the other hand, has clung to the traditional framework for the “range of military operations” as the defining framework for inter-state conflict, which leaves out the organizations, programs, and people in the United States that develop, deploy, and sustain our military forces for their use. Our adversaries have exploited this seam, the liminal zone, with great results. The figure below shows the zone at which most of our adversaries seek to operate.

Both China and Russia evolved their doctrines following the 1996 Taiwan Strait Crisis and collapse of the Soviet Union, respectively, to focus on the effective and efficient use of national resources to achieve national aims without provoking the United States into action. China’s recent behaviors in the Western Pacific and the challenges they prevent for operating conventional military forces can be seen as the culmination of a successful campaign in the liminal zone to raise the capability and quantity of China’s military forces to parity with the United States. Russia, while still weak, has exploited other liminal operations and tested under battlefield conditions in Estonia, Georgia, Syria, and Ukraine, in addition to other countries.

China, Russia, and other minor adversaries have shown repeated use of several tactics, which are found frequently as nations, corporations, organizations, and people maneuver in the liminal space. These tactics fall short of the traditional American view of the range of military operations but have significant impact on the capability and readiness of our forces, both now and in the future. These tactics can directly impact acquisition operations and place current and future programs and their systems at greater risk.

The tactics used generally run from clandestine operations to covert or ambiguous actions in the liminal space. Some tactics, if used too aggressively or overtly, may lead to immediate attribution and a proportional or escalatory response from the United States. Current, observable tactics in use by adversary nations include cyber warfare, industrial espionage and intellectual property theft, supply chain disruptions or compromise, lawfare, exploitation of humans, and information operations. Some of these tactics have been combined by adversaries to achieve specific objectives: rapid technological advancement and military modernization, sowing of distrust in program efficacy, and more. Acquisition warfare, as a concept, focuses primarily on the liminal actions and forgoes the impact of clandestine operations--the objective is to eventually provide program managers with a framework to actively defend against and counter adversary tactics that they can “see.” Clandestine activities, while assessed to be ongoing, are primarily the domain of law enforcement and the intelligence community and generally only rise to the level of visibility for program managers and staff when the threat transitions to insiders, cyber-enabled access, etc. Thus, we define acquisition warfare as:

Acquisition warfare is the set of tactics, operations, and campaigns to disrupt, delay, or deny an adversary effective research, development, production, or sustainment of current or future

capabilities by means of clandestine and liminal actions designed not to elicit a response from the target nation.

Some may argue that acquisition warfare is simply Phase Zero operations by another name. However, the use of Phase Zero terminology conjures legacy definitions of military actions to shape the battlespace: peacetime deployments, presence operations, humanitarian assistance and disaster relief, community relations projects, etc. Phase Zero is focused on operations external to the United States. Joint Doctrine Note 1-19 introduced the competition continuum, which begins to describe parts of the framework introduced under acquisition warfare as "competition below armed conflict," though the broader scope focuses on the whole of nation—vice government—approach (*Competition Continuum [JDN 1-19]*, 2019). Acquisition warfare differs from traditional Phase Zero operations in that it necessarily includes a whole of government approach that is focused on defending future programs and systems, not influencing existing international relationships and operations today. Additionally, it aims to provide program managers with the necessary platform and agility to respond to changes in the acquisition environment.

Adversary Campaigns and Tactics

Acquisition warfare consists of several common tactics that adversaries bundle into short-term operations or longer-term campaigns to achieve a specific objective against a U.S. acquisition effort or to positively advance their own developmental programs. These tactics include cyber warfare, industrial espionage, supply chain disruption and compromise, lawfare, exploitation of people, and information operations.

China is the most prolific adversary in this space, and an ongoing analysis from the Center for Strategic and International Studies highlights the severity and widespread nature of these campaigns. The findings are worth quoting at length to show the complexity of the campaigns. The statistics represent 160 cases from 2000 to the present only in the United States and exclude more than 1,200 cases of intellectual property litigation against Chinese companies.

For those cases where we could identify actor and intent, we found:

- 42% of actors were Chinese military or government employees.
- 32% were private Chinese citizens.
- 26% were non-Chinese actors (usually U.S. persons recruited by Chinese officials).
- 34% of incidents sought to acquire military technology.
- 51% of incidents sought to acquire commercial technologies.
- 16% of incidents sought to acquire information on U.S. civilian agencies or politicians.
- 41% of incidents involved cyber espionage, usually by State-affiliated actors.
- This list is derived from open-source material and likely does not reflect the full number of incidents. Of the 160 incidents, we found that 24% occurred between 2000–2009 and 76% occurred between 2010–2021 (*Survey of Chinese Espionage in the United States Since 2000*, 2021).

In 2018, the Office of the Director of National Intelligence published a report on Foreign Economic Espionage in Cyberspace that described holistically the Chinese campaign and objectives for economic espionage: develop comprehensive national power, an innovation driven economic growth model, and rapid modernization of the military (*Foreign Economic Espionage in Cyberspace*, 2018).

Russian activities tend to be more focused on cyber warfare and information operations to generate effects at the national, vice defense, levels, such as the interference with the U.S. presidential elections in 2016 and the prolific use of botnets to further polarize the American electorate, with the resulting emergent effects rippling into the defense program ecosystem in the form of greater budget uncertainty, among others (Badawy et al., 2018). Though the two countries are unlikely to be cooperating closely in conducting acquisition warfare campaigns against the United States, the variability of adversary campaign tactics highlights the dynamic, multi-front nature of acquisition warfare.

Cyber Warfare

Cyber warfare is not strictly a military activity, as China's actions have shown and as Russia's use of cyber warfare in integrated campaigns has highlighted in recent years. From a U.S. national perspective, cyber warfare presents a direct threat to U.S. critical infrastructure that we rely on to support program ecosystems: the power grid, water and sanitation systems, health care, consumer good supply chains, and others (Genge et al., 2015) Many adversaries are active in this space, and the last few years have witnessed several non-state actor cyber campaigns against U.S. critical infrastructure and cleared defense contractors (*Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013*, 2021; *Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology*, 2022; *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, 2022). The Colonial Pipeline attack was the most recent and most public example of this, but other attacks from a drone on a power substation and poisoning of water systems have also happened in the last few years (Greenberg, 2021; Trevithick, 2021; Turton & Mehrotra, 2021).

From a program perspective, cyber warfare tactics and operations are key enablers to facilitate other objectives, whether the theft of intellectual property or plans, insertion of malicious code into weapon systems, or gaining of information to blackmail and compromise cleared personnel. The Cybersecurity & Infrastructure Security Agency, in conjunction with the National Security Agency and Federal Bureau of Investigation, provides detailed information on several nation-state actors conducting cyber warfare against the United States, in some cases including detailed descriptions of specific tactics and operating patterns.

In acquisition warfare, cyber operations may not be direct attacks against military weapon systems while deployed, but rather the deliberate compromise of program networks or supporting software (e.g., NotPetya, SolarWinds, Log4j, Microsoft Exchange, etc.) and hardware for the purposes of compromising the system before it is deployed, or to concurrently developed tailored countermeasures against our systems. While this largely falls under the new umbrella of program protection today, current program protection efforts do not fully account for the cyber-attack surface that critical program information is exposed to. In 2019, the Secretary of the Navy commissioned and released a Cybersecurity Readiness Review, which gives an accurate and likely little-changed picture of the current state of Navy defenses against this element of acquisition warfare (*Secretary of the Navy Cybersecurity Readiness Review*, 2019). Most likely, latent malware has been placed in every penetrated system that may be activated in the run-up or beginning of hostilities. This malicious infrastructure has likely already compromised much of the program ecosystems.

Industrial Espionage

Industrial espionage may be effected through cyberspace, physical access, human exploitation, or a combination of means. From a program ecosystem perspective, this manifests as the intrusion and exfiltration of controlled unclassified program and technical information, contractor proprietary information, and compromise of classified networks for the same. This

may be done through cyber means such as compromising the network to gain access to sensitive information, insider threats to steal information, overt solicitation of key individuals with critical subject matter expertise through blackmail or job recruitment (the Thousand Talents program), and acquisition of specific corporations or their parent companies to gain access to sensitive information ("Committee on Foreign Investment in the United States Annual Report to Congress," 2020; Nakashima & Sonne, 2018).

Supply Chain Disruption

Over the last few decades, globalization and technological advances in information technology, manufacturing, and cost control have driven supply chains to be 1) increasingly global, 2) just in time, and 3) brittle in the face of disruption. As the COVID-19 pandemic proved, lack of inventory is only one factor that can cause disruptions to supply chains. In the case of the national security ecosystem, supply chains are those that furnish the systems in development and deployment, the items necessary for the program to complete their mission, including the business and IT environments, and the local supply chains that ensure that the workforce has their basic needs met, both personally and for their family, and thus can contribute and focus fully in the work environment. Supply chain challenges have grown to the point that in February 2021, President Biden signed Executive Order 14017 to establish the Supply Chain Disruption Task Force to address six national critical supply chains (*Executive Order on America's Supply Chains*, 2021)

Program managers cannot control the local supply chains, but they do have significant stake in the operation, resiliency, and efficacy of the supply chains that enable program action and the systems they deploy. Frequently, defense program offices and their contractor program office counterparts have little visibility into the program's overall supply chain below the first tier or two of subcontractors (Nothacker, 2021). Program managers must understand how adversary actions against supply chains impact the cost, schedule, and performance of the programs under management. In recent years, China, especially, has forcefully disrupted supply chains through campaigns to control certain sectors of the market, such as rare earth metals, compromise manufacturing supply chains to enable future access through cyber means to gain access to the program ecosystem (Dreyer, n.d.; Robertson & Riley, 2021). Given the extensive Soviet infiltration of the United States during the Cold War, the program ecosystem should be considered compromised already and subject to exploitation at the adversary's desire (Zhuk, 2022).

Lawfare

First defined by retired Air Force General Charles Dunlap in 2008, lawfare is "the strategy of using--or misusing--law as a substitute for traditional military means to achieve a warfighting objective." While normally exploited by non-state actors, non-governmental organizations, and others specifically to address human rights violations and similar issues, the tactics have come into increasing use to achieve various effects. China, naturally, has a widespread lawfare campaign to secure territory in the South China Sea (the Nine Dash Line and anchoring it to international law is a classic example of lawfare). Russia, as well, has used lawfare successfully to hold off the United Nations and other international bodies to allow it to act unencumbered in Crimea, Georgia, Estonia, and other states. At the corporate level, the exploitation of people for the Thousand Talents programs can bring the full weight of Chinese financial and legal resources to bear to tie a company up in expensive litigation over trade secrets, intellectual property, etc.

From an acquisition warfare perspective, lawfare targets individuals and corporations. Within each program ecosystem, there are certain individuals, whether key leadership or subject matter experts, who, if forced to leave the program, could significantly affect the ability of the

program to develop, deliver, or sustain capabilities. For example, if there are a few key scientists who understand hypersonics and are critical to the ongoing development programs, their departure could place the program at undue risk. Through other means, China or other adversaries may have accumulated sufficient information, such as from information operations, cyber warfare (i.e., the Office of Personnel Management data breach), and others, to create and proffer false claims and charges against individuals, thus embroiling them in legal battles and significantly degrading their productivity and leadership within the program ecosystem. Russia recently demonstrated a similar use of lawfare in the lawsuits against several computer security researchers who had worked to expose the connections of Alfa Bank, and Russian Bank, to President Donald Trump's campaign organizations (Devlin, 2021). Such use of lawsuits, similar to the rising prevalence of doxxing in American culture today, may have a chilling effect on the ability to research and attribute cyber-attacks or other actions in the future (Calabro, 2018).

Human Exploitation

China, again, is the most prolific adversary exploiting American workers for gain. All intelligence services continue clandestine operations to use insiders, recruited agents, and others to steal secrets (*The China Threat — FBI*, n.d.). China goes further. Much further. Originally starting with the Thousand Talents Program to bring overseas knowledge and talent into the Chinese domain, the efforts expand across nearly all sectors, ministries, and organizations and at the national, regional or provincial, and corporate levels to comprise 43 programs at the national level and more than 200 at lower levels (*CSET Chinese Talent Program Tracker*, n.d.).

These are rarely clandestine activities. As Nicholas Eftimiades (2020) reports, most of the human exploitation activities are conducted openly, with minimal to no espionage tradecraft, and with overtly stated objectivesClick or tap here to enter text.. This is the recruitment of people from academia, corporations, and government to provide information or services to China, share research or plans with China first, or simply move to China to work in a company, laboratory, or university there for higher pay. Many are Chinese nationals operating without cover names or stories and are conducting business openly, but one in four are American citizens recruited by Chinese officials. Defense programs and especially their supporting contractors are key targets given the industries we are involved in and the advanced technologies we work with.

Cultivation of a potential source often begins with a combination of information operations through social media and cyber activities to gain a better understanding of who the best targets for recruitment may be. Personnel advertising an active security clearance and program affiliation on LinkedIn may become targets for increased information gathering to allow for an eventual approach and recruitment, as happened to a former CIA officer (*Clearance Holders Targeted on Social Media*, n.d.).

Information Operations

All adversaries conduct information operations for the purpose of enhancing their own international stature or capabilities or degrading U.S. capabilities. This normally manifests in news articles, botnets to shape algorithmic search and filters, and campaigns to publicize new capabilities, but can also include the lower-level actions of pressuring U.S. companies to comply with Chinese laws if they serve or have business in China—think of YouTube, Facebook, and Google, for example, having to adjust software to prevent access to certain sites, as captured by Peter Singer and Emerson Brooking (2019) in *LikeWar*Click or tap here to enter text..

In the acquisition warfare space, this primarily comes out as creating immense pressure on the American acquisition system and its people through a sense of being behind Chinese, Russian, or other adversary capabilities in a particular area. The announcements of test results

for hypersonic anti-ship cruise mission tests, fractional orbital bombardment systems, or earlier operational capability deployments of unmanned systems, etc. have allowed our adversaries to use other elements of the national security-industrial complex and American media to put pressure on acquisition programs to deliver, which compounds with high-profile test failures or other program setbacks as the individuals in the program ecosystem seek to reap more benefits or resources than the ecosystem can reasonably or sustainably provide at that time (Hitchens, 2021; Newdick & Rogoway, 2021; Pollack, 2022; *Russia Test-Fires New Hypersonic Tsirkon Missiles from Frigate, Submarine*, 2021).

Conclusions and Areas for Future Research

This paper sought to unify the ongoing frustrations with defense acquisition reform and accelerating great power competition by, first, framing defense acquisition reform as a super wicked problem and, second, proposing the novel framework of the program ecosystem and acquisition warfare to provide a new lens from which to shape future actions at all levels of the defense acquisition ecosystem. The program ecosystem model provides a first attempt at describing the systemic forces that drive the behaviors of the program ecosystem. That understanding may yield new insights into how proposed changes will drive ecosystem behaviors and identify more optimal points for effecting change to achieve a desired outcome. As Levin et al. (2012) identify for global climate change, understanding a problem with super wicked characteristics will help policymakers better identify the solution sets that will be both palatable to other actors in the ecosystem and achievable within the current operating characteristics of that ecosystem.

Acquisition warfare and the program ecosystem, as a new concept, offer a multitude of avenues for future research. For program managers, adapting acquisition warfare and developing a program-specific ecosystem model, preferably through ethnographic and other forms of research to develop a functional casual loop diagram or dynamical model, will allow for a better understanding of the program's overall attack surface and help identify the limits of the program manager's influence over various behaviors in the ecosystem. Further research is needed to better identify and document adversary campaigns and their impacts on programs and tracing out the effects of those campaigns through the program ecosystem model to highlight the dynamism of them. The growing analytical capabilities in the field of network science will provide insight into network dynamics and help inform potential changes to the sociotechnical design of the ecosystem. The possibilities for future research in this new field are extensive.

References

Advisory Panel on Streamlining and Codifying Acquisition Regulations Volume 3 of 3 Summary of Recommendations. (2019).

Arkes, H. R., & Ayton, P. (1999). The sunk cost and Concorde effects: Are humans less rational than lower animals? *Psychological Bulletin*, *125*(5), 591. https://doi.org/10.1037/0033-2909.125.5.591

Badawy, A., Ferrara, E., & Lerman, K. (2018). Analyzing the digital traces of political manipulation: The 2016 Russian interference Twitter campaign. *Proceedings of the 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM 2018)*, 258–265. https://doi.org/10.1109/ASONAM.2018.8508646

Berenson, D. (2021). *The evolving geography of the U.S. defense industrial base - War on the rocks*. War on the Rocks. https://warontherocks.com/2021/09/the-evolving-geography-of-the-u-s-defense-industrial-base/

Burch, W. R., Machlis, G. E., & Force, J. E. (2017). *The structure and dynamics of human ecosystems: Toward a model for understanding and actions*. Yale University Press.

Calabro, S. (2018). From the message board to the front door: Addressing the offline consequences of race- and gender-based doxxing and swatting. *Suffolk University Law Review*, *51*. https://heinonline.org/HOL/Page?handle=hein.journals/sufflr51&id=65&div=&collection=

Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013. (2021, July 21). CISA. https://www.cisa.gov/uscert/ncas/alerts/aa21-201a

Clearance Holders Targeted on Social Media. (n.d.). Retrieved March 29, 2022, from https://www.fbi.gov/investigate/counterintelligence/the-china-threat/clearance-holders-targeted-on-social-media-nevernight-connection
Committee on Foreign Investment in the United States Annual Report to Congress. (2020). In *Committee on Foreign Investment in the United States*. https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2020.pdf
Competition Continuum (JDN 1-19). (2019). https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_19.pdf
CSET Chinese Talent Program Tracker. (n.d.). Retrieved March 29, 2022, from https://chinatalenttracker.cset.tech/
Department of Defense Report State of Competition within the Defense Industrial Base. (2022). https://media.defense.gov/2022/Feb/15/2002939087/-1/-1/1/STATE-OF-COMPETITION-WITHIN-THE-DEFENSE-INDUSTRIAL-BASE.PDF
Devlin, B. (2021, November 18). Alfa Bank lawsuits, Sussman indictment reignite battles over Trump organization computer links.. *The Washington Post*. https://www.washingtonpost.com/national-security/alfa-bank-trump-russia-sussman/2021/11/18/b10e498c-4726-11ec-b8d9-232f4afe4d9b_story.html
DoDD 5000.01 The Defense Acquisition System. (2020). DoD. https://www.esd.whs.mil/DD/.
Dreyer, J. T. (n.d.). *China's monopoly on rare earth elements—and why we should care*. Foreign Policy Research Institute. Retrieved March 29, 2022, from https://www.fpri.org/article/2020/10/chinas-monopoly-on-rare-earth-elements-and-why-we-should-care/
Dwyer, M., Tidwell, B., & Blivas, A. (2020). *Cycle times and cycles of acquisition reform.* Center for Strategic and International Studies. https://www.csis.org/analysis/cycle-times-and-cycles-acquisition-reform
Eftimiades, N. (2020). *Chinese espionage: Operations and tactics*. Vitruvian Press.
Executive Order on America's Supply Chains. (2021, February 24). https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/
Foreign Economic Espionage in Cyberspace. (2018). https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf
Fox, J. R., Allen, D. G., Lassman, T. C., Moody, W. S., & Shiman, P. L. (2011). Defense acquisition reform 1960-2009: An elusive goal. In *Defense Acquisition Reform*. Center of Military History, United States Army.
Genge, B., Kiss, I., & Haller, P. (2015). A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection*, *10*, 3–17. https://doi.org/10.1016/J.IJCIP.2015.04.001
Greenberg, A. (2021). *A hacker tried to poison a Florida city's water supply, officials say.* Wired. https://www.wired.com/story/oldsmar-florida-water-utility-hack/
High Risk Area - DOD Weapon Systems Acquisition. (n.d.). In *GAO High Risk List*. GAO. Retrieved March 26, 2022, from https://www.gao.gov/highrisk/dod-weapon-systems-acquisition
Hitchens, T. (2021, November 29). *It's a FOBS, Space Force's Saltzman confirms amid Chinese weapons test confusion*. Breaking Defense. https://breakingdefense.com/2021/11/its-a-fobs-space-forces-saltzman-confirms-amid-chinese-weapons-test-confusion/
Jang, W. J., Sanders, G., & Holderness, A. (2021, December 2). *2021 defense acquisition trends: Topline DoD trends after a half decade of growth.* Center for Strategic and International Studies. https://www.csis.org/analysis/2021-defense-acquisition-trends-topline-dod-trends-after-half-decade-growth
Levin, K., Cashore, B., Bernstein, S., & Auld, G. (2012). Overcoming the tragedy of super wicked problems: Constraining our future selves to ameliorate global climate change. *Policy Sciences*, *45*(2), 123–152. https://doi.org/10.1007/S11077-012-9151-0
Lineweaver, C. H., Davies, P. C. W., & Ruse, M. (2013). What is complexity? Is it increasing? In *Complexity and the Arrow of Time*. Cambridge University Press.
Margalef, R. (1963). American naturalist on certain unifying principles in ecology. *The American Naturalist*, *97*(897), 357–374.
Military and Security Developments Involving the People's Republic of China. (2021).
Nakashima, E., & Sonne, P. (2018). China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare. *The Washington Post*. https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html
Newdick, T., & Rogoway, T. (2021, December 14). *Russia unveils stealthier version of its S-70 "Hunter" unmanned combat air vehicle*. The Warzone. https://www.thedrive.com/the-war-zone/43504/russia-unveils-stealthier-version-of-its-flying-wing-unmanned-combat-air-vehicle
Nothacker, D. (2021). Supply chain visibility and exception management. In *Disrupting Logistics* (pp. 51–62). Springer. https://doi.org/10.1007/978-3-030-61093-7_5
Pollack, J. (2022, January 3). *Why do US hypersonic missile tests keep failing? They're going too fast*. Defense One. https://www.defenseone.com/ideas/2022/01/why-do-us-hypersonic-missile-tests-keep-failing-theyre-going-too-fast/360276/
Rapport, D. J., Regier, H. A., & Hutchinson, T. C. (1985). Ecosystem behavior under stress. *The American Naturalist*, *125*(5), 617–640. https://www.jstor.org/stable/2461475

Reichenberger, I. (2017). Digital nomads – A quest for holistic freedom in work and leisure. *Annals of Leisure Research*, *21*(3), 364–380. https://doi.org/10.1080/11745398.2017.1358098
Renewed Great Power Competition: Implications for Defense-Issues for Congress (Vol. 92). (2022). https://crsreports.congress.gov
Rittel, H., & Webber, M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*, 155–169. https://www-jstor-org.ezproxy2.library.colostate.edu/stable/4531523?seq=1#metadata_info_tab_contents
Robertson, J., & Riley, M. (2021, February 12). *Supermicro hack: How China exploited a U.S. tech supplier over years*. Bloomberg. https://www.bloomberg.com/features/2021-supermicro/
Russia test-fires new hypersonic Tsirkon missiles from frigate, submarine. (2021, December 31). Reuters. https://www.reuters.com/business/aerospace-defense/russia-test-fires-new-hypersonic-tsirkon-missiles-frigate-submarine-2021-12-31/
Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology. (2022, February 16). CISA. https://www.cisa.gov/uscert/ncas/alerts/aa22-047a
Secretary of the Navy Cybersecurity Readiness Review. (2019). https://www.wsj.com/public/resources/documents/CyberSecurityReview_03-2019.pdf?mod=article_inline
Serbu, J. (2021). *Pentagon's ponderous budget process is next target for Congressional reform.* Federal News Network. https://federalnewsnetwork.com/defense-main/2021/12/pentagons-ponderous-budget-process-is-next-target-for-congressional-reform/
Singer, P. W., & Brooking, E. T. (2019). *LikeWar: The weaponization of social media*. Mariner Books.
Survey of Chinese Espionage in the United States Since 2000. (2021). Center for Strategic and International Studies. https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000
Tadjdeh, Y. (2021, May 12). Just in: Pentagon 'doubling down' on acquisition reform. *National Defense Magazine*. https://www.nationaldefensemagazine.org/articles/2021/5/12/just-in-pentagon-doubling-down-on-acquisition-reform
The China Threat — FBI. (n.d.). Retrieved March 29, 2022, from https://www.fbi.gov/investigate/counterintelligence/the-china-threat
Trevithick, J. (2021). *Likely drone attack on U.S. power grid revealed in new intelligence report (Updated)*. The Drive: The Warzone. https://www.thedrive.com/the-war-zone/43015/likely-drone-attack-on-u-s-power-grid-revealed-in-new-intelligence-report
Turton, W., & Mehrotra, K. (2021, June 4). *Colonial pipeline cyber attack: Hackers used compromised password*. Bloomberg. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password
Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure. (2022, January 11). CISA. https://www.cisa.gov/uscert/ncas/alerts/aa22-011a
Vergun, D. (2021, May 14). *Acquisition reform is making rapid progress, defense official says*. DoD. https://www.defense.gov/News/News-Stories/Article/Article/2607639/acquisition-reform-is-making-rapid-progress-defense-official-says/
Welter, T. (2021, May 6). We are lost in the woods on acquisition reform. *Defense News*. https://www.defensenews.com/opinion/commentary/2021/05/06/we-are-lost-in-the-woods-on-acquisition-reform/
Zhuk, S. I. (2022). *KGB operations against the USA and Canada in Soviet Ukraine, 1953-1991*. Routledge.
Zinsstag, J., Schelling, E., Waltner-Toews, D., & Tanner, M. (2011). From "one medicine" to "one health" and systemic approaches to health and well-being. *Preventive Veterinary Medicine*, *101*(3–4), 148–156. https://doi.org/10.1016/J.PREVETMED.2010.07.003

Acquisition Research Program
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net