

Asymmetric Competition in the Arctic

Implications for North American Defense and Security

DR. LILLIAN “DOC” ALESSA

CDR JAMES VALENTINE, USCG, RET.

CDR SEAN MOON, USCG, RET.

DR. ANDREW KLISKEY

Abstract

The current Arctic security environment is poorly characterized. In the past few years, it has been termed “a return to great-power competition” and now is oscillating around discussions of *hybrid threats* or *gray-zone warfare*. Whatever the term, these are methods and means designed to avoid notice, obscure intent and origin, and exploit the seams in the targets’ awareness and response capabilities. In this article we use the term *asymmetric competition* (AC) to describe such activities, which exist as a continuum of conflict below open warfare, rather than fitting neatly into the binary notion of war and peace. While many national security scholars and practitioners are aware of and concerned about the use of AC by the People’s Republic of China (PRC), the ability of the United States and its allies to detect and protect against such behavior is limited. At the same time, the PRC has demonstrated a growing interest in the Arctic due to the region’s geostrategic importance and has taken an unusually aggressive posture toward asserting and securing Beijing’s interests there. We conducted an initial assessment to detect the extent, types, and tempo of AC using the Strategic Intelligence Framework (SIF)—a systems science methodology—to identify PRC asymmetric competition activities in the North American Arctic. Our results suggest an ongoing and pervasive AC campaign. We offer that integrative frameworks like the SIF can assist the United States, its allies, and its partners in detecting and characterizing AC with the accuracy and precision required for the development of strategy, policies, and response.

Great-Power Competition, Gray-Zone Warfare, and Hybrid Threats: Everything Old Is New Again

The PRC and the Russian Federation (Russia) are challenging the economic, military, and cultural dominance of the United States in the post–Cold War era. A range of literature exists in the political science and international policy realms

rich with references to great-power competition (GPC), gray-zone warfare, and hybrid threats, which can be summarized as follows:

1. The United States remains the most powerful conventional warfare force on the planet, with the greatest global reach;
2. Opposing the United States using direct military force in a geostrategic context is a dangerous and costly approach, with little chance of success, until hard-power parity is achieved; and
3. Those seeking increased national and global power at the expense of the United States will pursue indirect strategies (e.g., gray-zone warfare) and low-signature tactics (hybrid threats) designed to avoid detection, provide plausible deniability, and fall below thresholds that would trigger security/defense and protective responses.

However, this GPC is only new in the sense that it represents a change from the immediate past. The unquestioned dominance of the United States from the fall of the Soviet Union until today, or even the bi-polarity of the Cold War, and the clear emphasis on both the use and avoidance of conventional military engagement are the historical anomalies. Most human conflict has been something much less than all-out war, instead waged using many other methods.¹ This is something US policy makers previously recognized. One architect of post-World War II security, George Kennan, described it as *political warfare*, which he defined as “the employment of all the means at a nation’s command short of [hot] war, to achieve its national objectives.”² In this article, to avoid the morass of terms and their previous or competing definitions, we refer to all these linked concepts collectively as *asymmetric competition* (AC), since the underlying principle is to avoid head-to-head competition using matching hard-power elements. We further define *threat* as some activity or action that gives the actor advantage, preferably at the expense of the target.

Asymmetric Competition as Geostrategic Environment Shaping

Since the end of World War II global norms have been rooted in what are usually termed liberal, internationalist ideas. This includes the concepts of universal human rights, freedom of the press, equality before the law, a representative form of government, and various civic freedoms. These ideas are liberal in the sense that they emphasize that individuals have certain intrinsic rights that cannot be morally or ethically violated by others—including the state. These ideas are internationalist because these asserted rights attach to the person, rather than ruled territory, and nations are expected to uphold them. For example, the United Nations’ Universal Declaration of Human Rights states that all people, everywhere, are “entitled to a

social and international order in which the rights and freedoms set forth in this Declaration can be fully realized.”³ Similarly the North Atlantic Treaty Organization (NATO) embraces these standards in its opening articles, and the International Criminal Court was explicitly founded to try cases where a country fails to act on its own, or is “in reality . . . unwilling or unable” to do so.⁴ While the actual exercise of such ideals is never perfect, these basic principles form the foundation of existing global norms and standards for state behaviors.

Challenging these norms can—and often does—create internal and international backlash and consequences, even if they are applied unevenly. These range from internal protests (e.g., Hong Kong 2019–2020), to coercion through sanctions or military force up to and including full-scale invasions. In many ways this runs counter to a strict Westphalian construction, which emphasizes the absolute right of each state to be the “sole author of laws within its jurisdiction . . . hold a monopoly on the organized use of force,” and regards influence or interference in the domestic affairs of a state as a violation of sovereignty so severe it may prompt open war.⁵

The PRC and Russia are primarily authoritarian in their rule, and thus potentially subject to various negative consequences should their actions violate these standards. Both countries would naturally prefer a more permissive environment, where, for example, the PRC’s Uighur genocide, or its handling of Hong Kong, were not grounds for repercussions.⁶ As neither Russia nor the PRC can yet reasonably challenge the hard power of the United States, Moscow and Beijing seek to revise the existing rules in ways that favor their national and global objectives while simultaneously undermining current norms, institutions, and those that support them using “all the means at a nation’s command.”⁷ Some authors have attempted to reframe the PRC’s actions as more complex than revisionism, but none of the presented arguments adequately explain things like the prohibition on researching “Western constitutional democracy, universal values of human rights, Western-inspired notions of media and civil society independence . . . neoliberalism, and ‘nihilistic’ critiques of the state,”⁸ the PRC’s pursuit of dissidents abroad, or its use of “sharp” power to erode trust in government and societies through censorship, dis- and misinformation, and interference in sociopolitical relationships and institutions that involve academia, culture, media, and economies (ACME). The latter has grown so strong so that even non-Chinese academics report self-censorship to avoid PRC entanglements.

Asymmetric Competition as National Strategy

The examples above demonstrate the PRC’s strategy for reshaping the political and security environment. In 1999 two senior PRC military officers wrote *Unrestricted Warfare*, explaining how the PRC could defeat the militarily superior

United States by using other elements of national power and avoiding direct engagements.⁹ The “Three Warfares” outlined in the book—psychological warfare, public opinion warfare, and legal warfare—have since been elevated to official PRC doctrine. Salient examples include: the use of “business, technology and science, education, culture and tourism,” as official state tools to achieve national objectives; laws that assert extraterritorial jurisdiction over PRC critics, including noncitizens; cyberattacks; coercive “debt diplomacy”; exportation of surveillance and social credit technology to other nations; use of China’s fishing fleet as a naval militia; and sharp power aimed at CAMP targets. Despite their security implications, few of these events trigger security responses under most national or international rule sets. These events exist in a “gray zone” of conflict—neither open war nor innocent coincidence—where the right response is unclear and the line between “regular” and threatening acts is blurred. Thus, AC is designed to take advantage of the seams in institutional awareness and response thresholds. The practical effect is that disaggregation of the “threat signal,” from the surrounding “normal” is a herculean task using existing methods—if they work at all.

Asymmetric Competition as Action

In direct implementation, AC consists of what are sometimes called *hybrid threats*. These threats combine multiple aspects of state power, and act below detection and response thresholds to achieve objectives. Recognition of such dangers as serious threats demanding national and mutual security options led to the establishment of the NATO European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in 2017. The Hybrid CoE provides a clear and concise definition of hybrid threats:

The term hybrid threat refers to an action conducted by state or non-state actors, whose goal is to undermine or harm the target by influencing its decision-making at the local, regional, state, or institutional level.

Such actions are coordinated and synchronized and deliberately target democratic states’ and institutions’ vulnerabilities.

Activities can take place, for example, in the political, economic, military, civil or information domains. They are conducted using a range of means and designed to remain below the threshold of detection and attribution.¹⁰

As a structural feature of liberalism—and by adversarial intent—this is an uncomfortable space for liberal states and institutions, which through their adherence to rule of law use legality as a proxy for what is threatening and what is not. The implication is that legal acts are not harmful, or at least not detrimental

enough to justify state intervention.¹¹ The Hybrid CoE notes that an “intensifying conflict of values” between liberal and authoritarian states, “an increasingly complex information environment,” and vulnerabilities inherent in open societies create a ripe strategic operating environment for hybrid actors, if left unchecked.¹²

Detection and Analysis of Asymmetric Competition is Lacking

AC below the nation-state level is difficult to detect, since these events have low-signature and are aimed at the seams identified above.¹³ Apart from the myriad information-sharing problems routinely lamented, or the treatment of analysis problems as though they are information-collection problems, there is the concern of analytic bias, in this case, what the US Intelligence Community (IC) calls “mirror imaging.” *Mirror imaging* is when analysts or organizations “project [their] thought process or value system onto someone else,” leading to mischaracterization and errors in estimative assessments. While the IC officially trains analysts to avoid mirror imaging, the practice remains pervasive throughout the community.¹⁴

This is a question of cognitive frameworks: information and data are evaluated through the lens of what is important, relevant, and sensible to the analyst/United States, rather than the analysis target. The result is a set of conclusions that are logical and internally consistent but may have no bearing on reality; “just because something seems logical to an analyst does not mean that the subject being analyzed will see it that way—especially when differences in thought processes and beliefs are factored into the equation.”¹⁵ Given that AC is explicitly employed to avoid *expected* confrontation points, it is easy to see how our intelligence enterprise has more often missed than detected it.

Methodology: Using the Integrative Frameworks of System Science to Detect and Characterize the AC Threat

To address these profound shortcomings in our broad intelligence processes, we used a systems science framework, in collaboration with diverse defense, security, and intelligence practitioners. The resultant Strategic Intelligence Framework (SIF) is an updated method for approaching intelligence problems using rule managers, diverse data ecosystems, data processing (analytics), and pattern development and relationships, here termed *pattern confluence* (e.g., analysis and conclusions), to detect AC. Developed in collaboration with agencies and personnel across the US and Canadian security and defense enterprises, the SIF is like an amplifier and noise reduction circuit in an electronic device. It boosts the targeted threat signals, while filtering out information that masks the target. Drawing from complex systems, mathematics, social science, and geographic information

science, the target signals are not analyzed in isolation but in relation to both their geographic context and each other. The result is a qualitatively and quantitatively accurate representation of the threat estimate. This provides clear, actionable, and precise strategic intelligence to consumers—something that remains sorely lacking for the Arctic.¹⁶

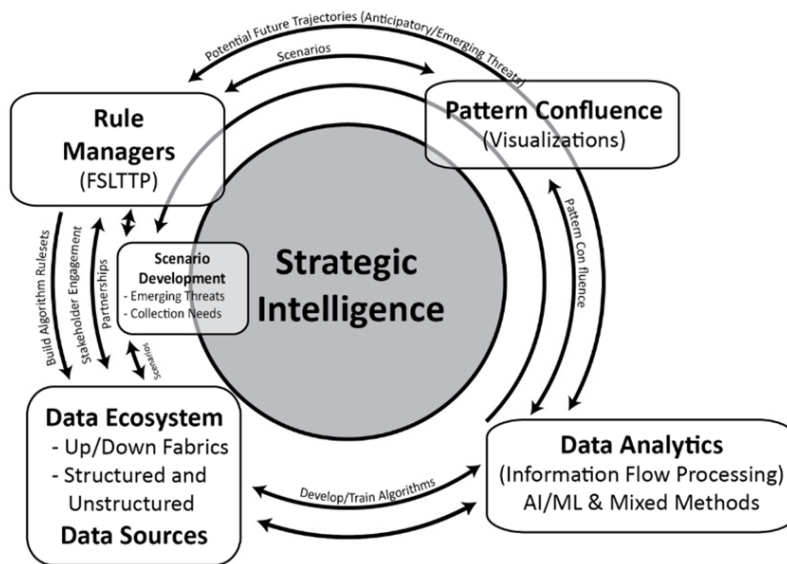


Figure 1. Strategic Intelligence Framework (SIF). FSLTTP refers to federal, state, local, territorial, tribal, and private partners. This graphic was developed with a large enterprise of connected organizations in mind. Data collection, algorithmic steps, analytics, and visualizations were executed manually in this research. (Alessa et al. 2021).

Challenge Question: Is the PRC Engaged in Asymmetric Competition in the North American Arctic?

Arctic Security Requires Integrated Analysis

As the Arctic changes and becomes more accessible, it has gained increased defense and security attention. The US Department of Defense (DOD), for instance, published its Arctic strategy as a report to Congress in 2019, and academic literature on Arctic security has exploded over the past 10 years, with the number of annual articles approximately doubling between 2012 and 2020 (fig. 3).¹⁷ This is capped by a nearly 25-percent increase from 2019 to 2020. Examination of article subjects and publishing journals shows a body of work from the “usual suspects” in security and defense matters: topics such as geopolitics, international relations and law, sociology, and political science contained in regional political, policy, and military/defense journals. Environmental science occasionally appears but usually within the context

of human or social security in a warming Arctic. Broadly, there is great conceptual depth, topical analysis, and interdisciplinary research, well-supported within the analysis and theory of the humanities and their careful evidentiary standards. The Arctic is an “interstitial region” as defined by Dylan Craig, to which the Arctic nations are “institutionally committed” but within which their “conventional tools of warcraft and statecraft are excluded by both practical and legal considerations.”¹⁸ The highly variable climate, low population density, and lack of infrastructure mean that law enforcement, military forces, regulatory organizations, and emergency services are sparse. This is compounded by a complex legal and sociocultural terrain in which Arctic nations make competing claims, and the rights and historical practices of indigenous populations overlap and sometimes conflict with the desires or even borders of sovereign states.

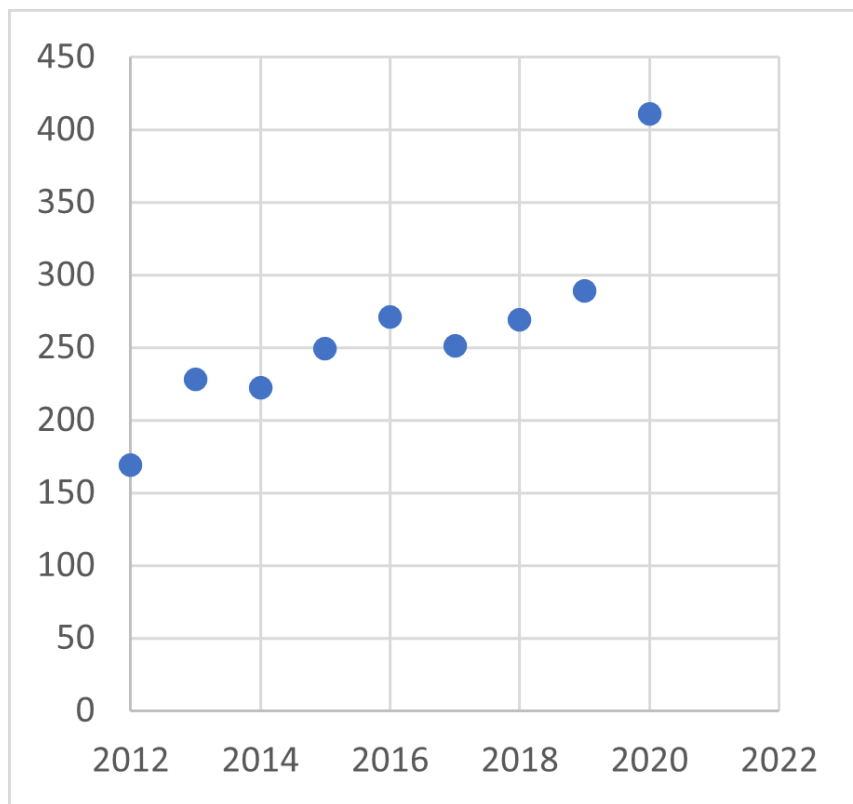


Figure 2. Arctic security. Peer-reviewed literature analysis for “Arctic Security” as the number of results per year.

These publication types and trends also mean that examinations of Arctic security are being made using methods that are qualitative, leading to highly generalized conclusions. Three main themes dominate existing Arctic threat narratives:

- An equipment and infrastructure “arms race” occurring between the United States and its allies, Russia, and the PRC;
- Concerns about militarization (e.g., Russian build up, etc.) or forms of cash diplomacy to gain access to the region (e.g., the Arctic Silk Road); and
- Prognostication of geopolitical dynamics and international affairs, based on any number of theories, and/or schools of thought.

If these are conducted by think tanks or contracted to the private sector, they often bear a substantial price tag to the US taxpayer. Realistically, none of these provide the degree of precision necessary to guide policy, workforce development, and resource acquisition such as targeted investment in technologies, education, or training, beyond “the Arctic has arrived as a policy problem and will require some kind of investment in these categories.” This is not a criticism of the humanities, think tanks, policy engines, or their adjacent fields. It is, rather, a recognition that data and information are not being leveraged for quantitative analyses to create better descriptive, explanatory, and predictive methods that serve operational needs and often by those far removed from not only the Arctic but also lacking the necessary expertise and skill sets. With that in mind, we apply the SIF here as just such an integrative method to analyze North American Arctic threats in the context of AC.

Rule Management, Scenario Creation

Through a meta-analysis of 12 workshops on Arctic security between 2017 and 2020, we established that many US and Canadian academic and practicing security experts are worried less about the hard militarization and financial footholds in the Arctic than apparent attempts by adversaries like Russia and the PRC to gain information, create local contacts and networks, “buy” influence and access, conduct tests of security measures, and other such activities. In practitioners’ views, such attempts are aimed at undermining local and national security. Often, practitioners expressed that what they were concerned about was perfectly legal, rendering law enforcement or criminal investigation moot. Their perspectives on this issue were often rooted in practical Arctic experience. For all the changes rendering the Arctic more accessible, it remains a remote region with significant barriers to military and other operations and logistics. So, while militarization was certainly a concern, they deemed the clearly described AC threats as being of greater immediate, strategic importance.

The study area for the North American Arctic was established as extending from the northernmost territory of the United States and Canada southerly to 51° N latitude—the most northern latitude that fully contains all Alaskan territory (fig. 3)

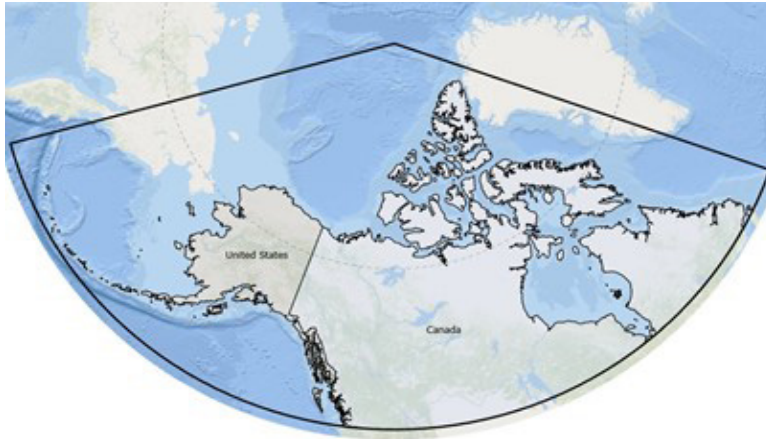


Figure 3. Study area. Starting at the North Pole and extending south to 51° N, to encompass the southernmost Aleutian Islands. Eastern and western boundaries include the Canadian-owned continental shelf (east), and the Komandorskiye Ostrova (Commander Islands), owned by Russia, which defines the westernmost Aleutian Islands.

Assumptions

Evaluation of PRC history, policies, doctrines, and strategic direction led to the creation of four evidence-based assumptions.

Assumption 1: The PRC's strategy for reaching national objectives is fundamentally different than that of liberal democracies. This includes conceptions about appropriate priorities, goals, objectives, institutions, and acceptable exercises of state power.

As an example, unlike Western democracies, which strive to divorce military and security institutions from politics, the PRC views such organizations expressly in political terms. This is established PRC political theory (e.g., Mao's declaration of the Red Army as a "mass propaganda" organ at the Gutian Conference) as well as practice: The first mission of the People's Liberation Army (PLA), which comprises the entire structure of the PRC armed forces, is to safeguard the Chinese Communist Party (CCP), while the second is to safeguard China.¹⁹ The PLA is additionally ordered to "actively participate in the country's economic and social construction, and firmly maintain social stability, so as to remain a staunch force for upholding the CCP's ruling position and a reliable force for developing social-

ism with Chinese characteristics.”²⁰ State-owned companies, and even the PRC’s fishing fleet and research vessels, are explicitly deployed for political objectives, and so forth.²¹ This conception of state security as an inherently political function is reflected by Beijing’s policy, strategy, and doctrine, as discussed above.

Assumption 2: Events undertaken by PRC entities, such as resource extraction, infrastructure development, and institutional participation are political acts designed to not only erode the existing liberal norms and standards of international relations and global security but also acquire precise data on a range of topics. These erosions threaten the security of the United States and its allies by limiting our defense options and expanding China’s.

Viewed as individual events, the actions taken by China are rarely, if ever, illicit or illegal. In aggregate, however, patterns emerge that provide greater insight into not only the breadth and diversity of ACME activities but also the interrelationships that reflect a sophisticated synergy. For example, broad collaborations across academia provide continuous open-source data and information feeds that can accelerate and target the acquisition of natural resources or strategic facilities. Built into this structure is a level of redundancy that, despite prognostications of China as an overextended house of cards, allows for multiple failures at any given time.

Assumption 3: The PRC is actively interested in the Arctic for security reasons.

Examination of PRC statements, actions, and policies reveals a steadily increasing interest in the Arctic since at least 2003, when Beijing established the Yellow River Arctic Station in Svalbard.²² Since then, the PRC has racked up an impressive list of accomplishments in the Arctic for a country with no Arctic territorial claims. In 2013, China became a permanent observer on the Arctic Council.²³ In 2016, the PRC constructed a satellite ground station in Kiruna, Sweden.²⁴ In 2017, Beijing suggested an “Arctic Silk Road” concept. In 2018, the PRC established a research station in Iceland and published China’s own Arctic policy.²⁵ The last is notable for declaring that the PRC is a “near-Arctic state”—a term with no legal status or weight.²⁶ The European Parliamentary Research Service (EPRS) described the PRC Arctic policy as intentionally ambiguous, designed to assure Arctic and Western nations that China intends to support and observe existing arrangements, and “more interesting for what it omits, such as the national security dimension that is a major driver of China’s Arctic ambitions.”²⁷

While the policy states that the PRC intends to pursue its goals in accordance with all relevant international law, it was also carefully crafted to directly

challenge the extant international norms that favor sovereign and regional governance of the Arctic in accordance with territorial claims in and around the Arctic Circle.²⁸ Of note are the PRC's interests in promoting tourism, infrastructure development, and respect for indigenous culture, rights, history, and self-rule. Each of these provides unique opportunities for the PRC to gain access to the Arctic; leverage PRC presence as an argument for participation in governance, security, and development arrangements; and engage directly with Arctic communities that possess various levels of autonomy.

Assumption 4: Open-source data will provide enough information to assess the nature and location of PRC AC events.

While intelligence communities and assessments frequently rely on, and accord higher status to, classified information and methods, the amount of openly available information simply dwarfs anything that can be collected via classified means. One National Geospatial-Intelligence Agency (NGA) director “argued that unclassified information should no longer be seen as supplemental to classified sources.” Rather “classified sources can be used to ‘supplement an ever broader and richer and unclassified base of knowledge.’”²⁹

Emerging Threat Identification and Scenario Analysis, Data Collection, and Rule Set Generation

Further examination of the PRC's 2018 Arctic Policy reflects that a key unstated purpose is ensuring the PRC's security and defense advantage, while word frequency analysis shows that “security” is barely mentioned (fig. 4).

However, processing the text by category or theme reveals that security plays a much greater role than the raw text suggests. To do this, each word in the policy was grouped into one of six thematic categories: access, development, governance, research, resources, and security. Words that did not carry an individual thematic meaning (e.g., belongs, endeavored, related, furthermore, shoulders, etc.) were removed from the data set. The frequency of the remaining words was used to examine the difference between the policy's stated and implied priorities using normalized scores (fig. 4 and tables 1, 2, and 3).



Figure 4. Word cloud generated from PRC Arctic Policy. This cloud eliminates common “stop words” (e.g., the, and, etc.) as well as “China,” “Arctic,” and “international.” Produced using Python Natural Language Toolkit 3.5 and Python WordCloud 1.8.1. The size of the font corresponds to the frequency of the word in the policy (max: 45, min: 1).

$$SP_{score} = \frac{\sum Word\ Frequency_{theme}}{\max \sum Word\ Frequency_{theme}}$$

Table 1. Stated priority score for PRC Arctic Policy

$\frac{\sum Word\ Frequency_{theme}}{max\sum Word\ Frequency_{theme}}$	Theme	$\sum Word\ Frequency_{theme}$	SP_{score}
	Governance	570	1.0000
	Knowledge	321	0.5632
	Access	302	0.5298
	Resources	186	0.3263
	Development	150	0.2632
	Security	107	0.1877

$$\bar{W}_f = \frac{\sum \text{Word Frequency}_{\text{theme}}}{\text{Theme Unique Word}_{\text{count}}}$$

and:

$$IP_{score} = \frac{\bar{W}_f}{\max \bar{W}_f}$$

Table 2. Implied Priority Score

$IP_{score} = \frac{\bar{W}_f}{\max \bar{W}_f}$	Theme	Unique Words	\bar{W}_f	IP_{score}
	Governance	94	6.1290	0.9398
	Knowledge	69	4.6522	0.7133
	Access	56	5.3929	0.8269
	Resources	31	6.0000	0.9200
	Development	23	6.5217	1.0000
	Security	21	5.0952	0.7813

The above equations use word frequency as a proxy for thematic importance. Equation 1 compares the total frequency of terms related to a theme to the maximum frequency for all themes to yield a normalized score. This provides a sense of the policy's stated priorities, as it is a straight comparison of frequency between themes. Equation 3 accounts for the unique words used for each theme, thus controlling for the quantity of different, but thematically related words, to arrive at an implied priority. The two figures are compared through what we have dubbed the "Janus Ratio," which compares what is *meant* versus what is *said* in the policy document. A value greater than one indicates the theme is a greater priority than stated, and the higher the value, the greater the discrepancy between the stated and implied priorities.

$$Janus\ Ratio = \frac{IP_{score}}{SP_{score}}$$

Table 3. Janus Ratio

$\frac{IP_{score}}{SP_{score}}$	Theme	IP_{score}	SP_{score}	<i>Janus Ratio</i>
	Governance	0.9398	1.0000	0.9398
	Knowledge	0.7133	0.5632	1.2667
	Access	0.8269	0.5298	1.5608
	Resources	0.9200	0.3263	2.8195
	Development	1.0000	0.2632	3.7990
	Security	0.7813	0.1877	4.1624

Based on the existing assumptions and policy analysis, the hypothesis for this study is:

The PRC is conducting AC in the North American Arctic in accordance with its Arctic policy. The purpose of these AC activities is to provide the PRC with a long-term, strategic advantage over both the United States and Canada in the Arctic theater while limiting our—and our partners' and allies'—defense options.

Data Needs and Rule Sets for Processing and Evaluation

The model for PRC behavior in the scenario was developed by stepping through three interrelated and well-established frameworks for military and national security analysis and planning: (1) ends, ways, and means; (2) the diplomatic, information, military, economic, financial, intelligence, and law enforcement (DIMEFIL) model of national power elements; and (3) the political, military, economic, social, infrastructure, information, physical environment, and time (PMESII-PT) variables of the relevant operating environment. Ends, ways, and means connects the desired end states to the methods and capabilities required to realize them; DIMEFIL describes the arsenal of tools nation-states use to achieve their ends; and PMESII-PT is the location and placed based knowledge (LPBK) that must be gathered for success (fig. 5).

These were applied to the scenario to answer the following question: If the scenario is true, and the PRC is using hybrid threats in the North American Arctic, what exactly would the PRC seek to accomplish, how would it attempt to reach its goals, what forms of national power would it exercise, and what would its target sets be? An existing relevant body of knowledge ranging from official PRC statements, policies, and history to news articles, academic treatments, and non-PRC official documents (US government, EPRS etc.) was analyzed using the frameworks identified above to identify logical themes about PRC goals, doctrine, employment of national power, and possible targets for AC in the North American Arctic operating environment. This guided both data and information needs (i.e., what to research and gather), as well as established characteristics that, when present in the aggregate, indicated that an event or activity posed a threat when examined in an AC context.

Data Ecosystem, Sources, and Analytics

Data for this research was both structured and unstructured, collected manually (webcrawlers and other automated methods were not used) from openly available sources between 2020 and 2021 and spans the period from 2005 to 2020.³⁰ The

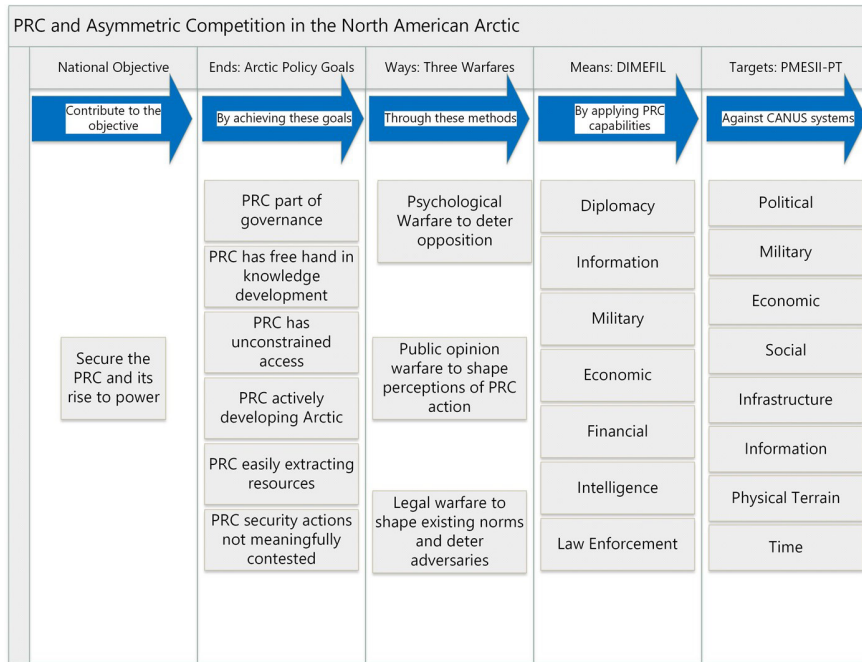


Figure 5. Development process for creating data needs and evaluation criteria

baseline for inclusion was some action taken by a PRC person, business, organization, or official within the study area. Data meeting these criteria were then subjected to the process in figure 6 (left-hand graphic). Personal blogs, social media, and other similar sites were not used to establish provenance. The types of data gathered and evaluated ranged from diplomatic and economic engagements to vessel positions, covering 73 unique events associated with 280 (non-unique) land coordinates and 17 vessel transits. These events were then scored (right-hand graphic, fig. 6), based on characteristics that, when present, indicated that the observed event carried a threat signature under the established scenario. These indicators included a range of considerations such as:

- How much access the event granted to gaining knowledge about, or altering, operating environment characteristics; for example, an oil well or mine is predicated on reams of geophysical, biophysical, hydrologic, cultural, legal, political, and other documentation.
- Direct connection to the PRC state apparatus through company ownership or other markers.
- Event alignment with the stated actions and elements of PRC strategic power exercise and objectives (e.g., tourism, resources, navigation/transportation, etc.).

- PRC use of methods previously identified in other places to extract a strategic power advantage (e.g., debt diplomacy, hacking, technology and infrastructure assistance, etc.)
- Actions that pitted the interests and desires of constituent components (communities, states, tribes, provinces, and so forth) against each other or the sovereign state.

Finally, each event was assigned a degree of estimative uncertainty based on a holistic examination of the event, its context, the actors involved, data quality and quantity, and other factors deemed relevant. This process mirrored the analytic standards of Intelligence Community Directive (ICD) 203 but was expressed as a quantitative (+/- percentage), vice a qualitative (approved “estimative language”) format.³¹

Pattern Confluence and Visualization

Collected information was visualized through commercial geospatial software (ArcGIS Pro 2.9). Vessel transits, expressed as ~180,000 time-ordered coordinates, were converted to line features then resampled at 100km intervals for spatial consistency prior to analysis. Each point then received a spatial adjustment to its score in accordance with figure 7. Locations inside the Arctic received the full weight of their score, while those outside the Arctic Circle were weighted by the ratio of the point latitude and the latitude of the Arctic Circle ($\frac{\text{Latitude}_{\text{Location}}}{66.5636}$). Maritime points received an additional spatial weighting based on whether the position was in the exclusive economic zone (EEZ), contiguous zone (CZ), or territorial sea (TS) of either the United States or Canada, each of which confer different rights and privileges to the controlling state.³²

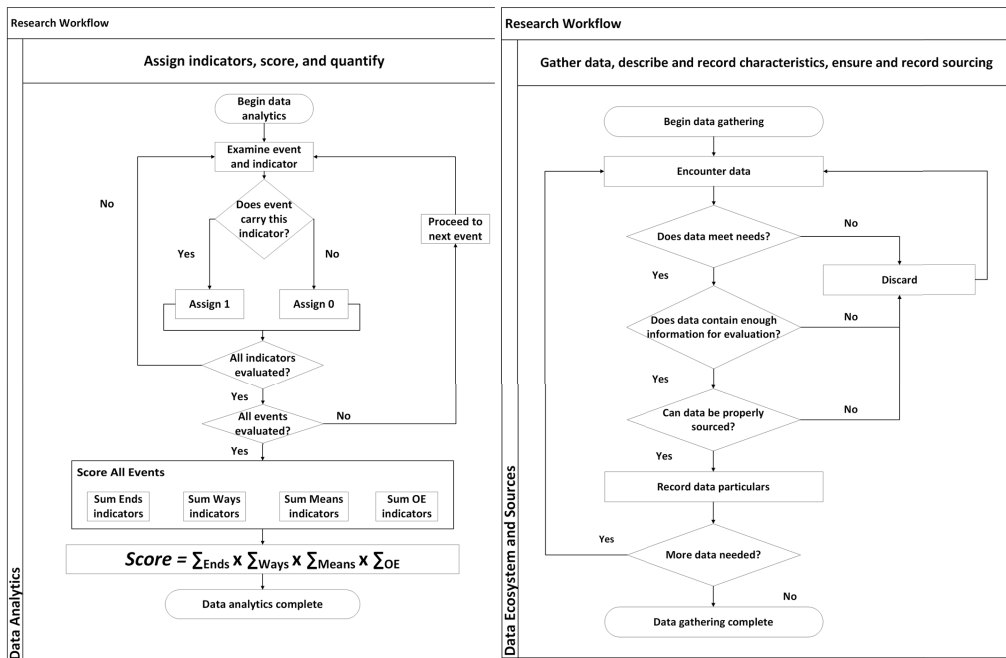


Figure 6. Research workflow. Data collection and inclusion process (left); Data scoring (right) based on the presence or absence of characteristics that were assessed to form the signature of PRC AC threats in the study area.

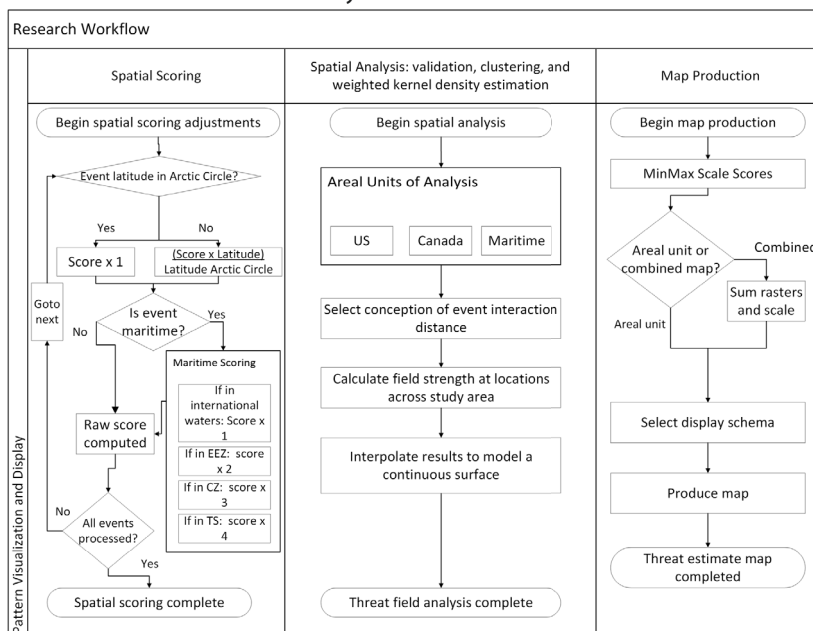


Figure 7. Spatial scoring, pattern creation, and visualization

Establishing Pattern Confluence through the Gravity Model of Spatial Interaction

The gravity model of spatial interaction rests on foundational premises of both geographic information analysis and complex systems theory: that the relevant pieces of a system impact every other piece of the system to a greater or lesser extent. Geographically, the strength of this impact is related to the distance between them. Military and security readers will note this is an expression of Boulding's Loss of Power Gradient, and more generally of Tobler's Law.³³ We treated each location as though it radiated a "threat field" from its center, which decreased in strength proportional to its distance. This conception of spatial interaction is called the *Gravity Model* as it bears resemblance to those of fundamental physical forces, such as gravity, electromagnetism, and so forth.³⁴ It follows that the threat in any location is the sum of the partial threat fields:

$$TF_{Location} = \sum_1^n \frac{Source_1}{d_{1 \text{ to } Location}} \dots \frac{Source_n}{d_{n \text{ to } Location}}$$

Where:

$Source_n$ is the threat score assigned to one of the analyzed events at location n ; $d_{n \text{ to } Location}$ is the haversine distance between the source location n and any point in the study area³⁵;

and,

$TF_{Location}$ is the "threat field strength" at any point in the study area.

Results: The Mesoscale Operational Situational Awareness Intelligence Composite (MOSAIC)

We selected a threat visualization that identified threat locations, the relative field strengths, and incorporated estimative uncertainty. The latter is critical for threat analysis but often unused apart from approved ICD 203 language. To accomplish this, we used equation 5 to calculate the threat field strength over an appropriately dense point grid to ensure spatial accuracy, and then interpolated between the grid points to model the strength of the threat field everywhere in the study area (figs. 8 and 9).

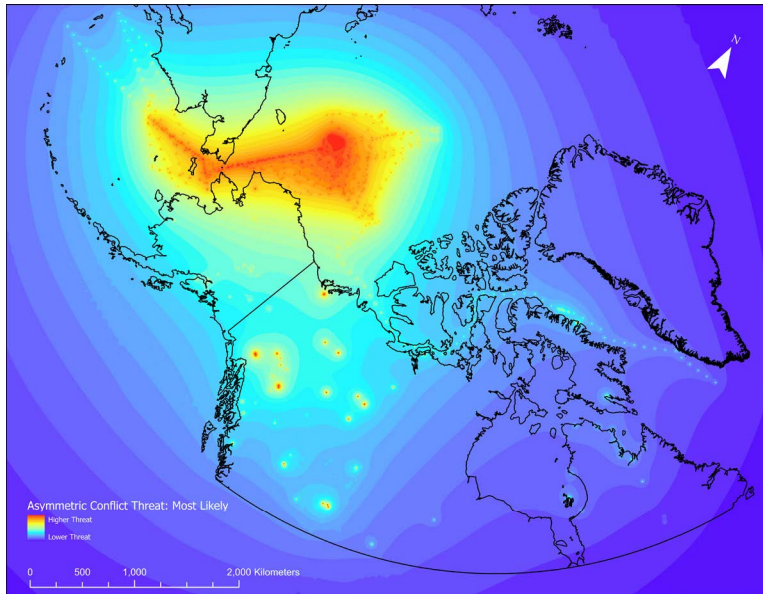


Figure 8. Most likely. The most likely state of the PRC asymmetric conflict threat in the North American Arctic.

By adjusting field strengths to account for uncertainty, we displayed a “best-case” and “worst-case” scenario map, where the threats were respectively as low and high as possible within the confidence bounds of the assessment (figs. 9 and 10). Because figures 8, 9, and 10 are geographically contextual representations of conclusions designed to provide awareness to national security consumers assembled with an integrative framework combining qualitative and quantitative methods, we call them Mesoscale Operational Situational Awareness Intelligence Composites (MOSAIC).

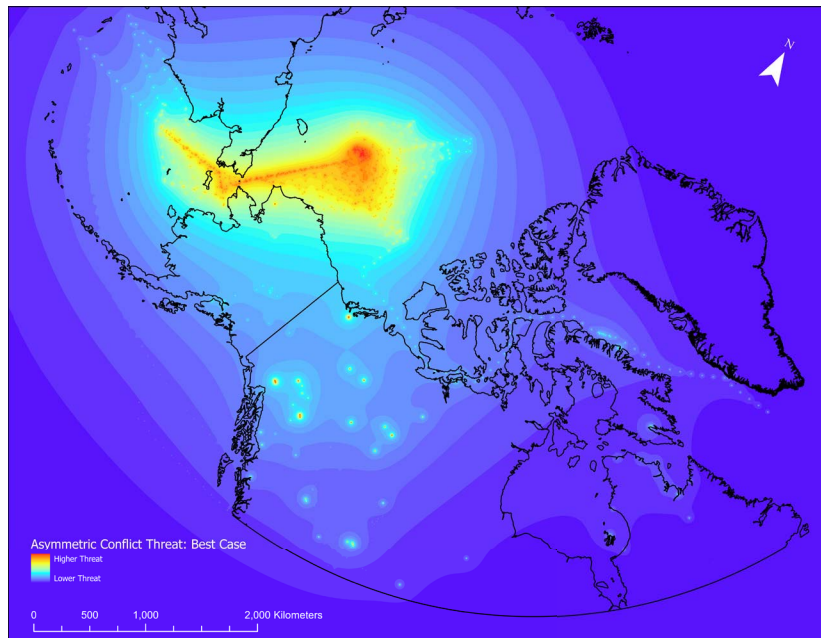


Figure 9. Best case. The best case for the state of the PRC asymmetric conflict threat in the North American Arctic.

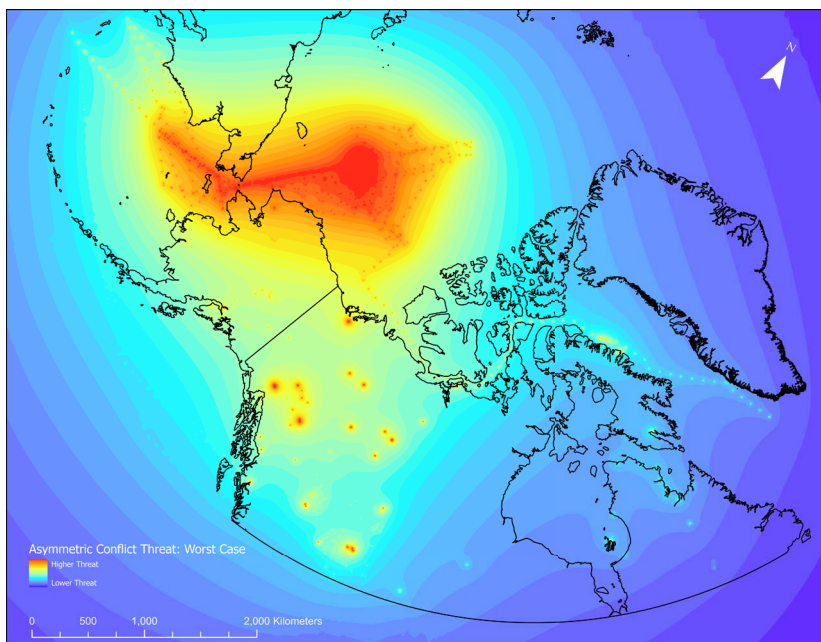


Figure 10. Worst case. The worst case for the state of the PRC asymmetric conflict threat in the North American Arctic.

The Arctic Is Experiencing a Sustained Level of Asymmetric Competition Activities

While the MOSAIC bears visual similarities to common “heat maps” created with spatial statistics, the differences in how they are calculated means that the MOSAIC provides a spatially and mathematically accurate map of estimative intelligence. It is, in essence, a georeferenced visualization of what analysts think about the threat. In this case study, three maps convey an intelligence research-and-analysis conclusion based on hundreds of (open) sources and a rigorous framework at least equal to, and certainly more integrative than, the structured analytic techniques taught and used in the US IC.³⁶ Furthermore, the MOSAIC accounts for and displays the impacts of estimative uncertainty in a quantitatively valid manner rather than relying on easily misused and misunderstood phrases inserted into findings.

The MOSAIC is also simply and rapidly updated. The evaluative rule sets are easily applied to new information, and the MOSAIC recalculated/revisualized. The integration of the data environment and sources into the SIF’s knowledge generation cycle allow them to be directly tapped and perpetually examined to ensure reliability and provenance both in part and in whole. Inspection of the MOSAIC by the rule managers can occur at any interval desired, providing feedback that improves or updates the scenario, data and sourcing, and evaluation rules. And—in what is perhaps a first in intelligence analysis—the SIF and MOSAIC provide a means of tracking accuracy and (one hopes) improvement over time: the results of the SIF and MOSAIC process at any time, in any location, can be compared to a “ground truth” established by a complete interdisciplinary, inter-agency investigation of selected events.

While such studies have been conducted previously, they were usually “post-mortem” looks at intelligence conclusions, driven by crisis or surprise, that compare a now-known negative consequence to the information that might have been used to predict or prevent it. Here, the analysis conclusions about any event—in this case, is it or is it not an instance of AC—can be thoroughly vetted before final and irrevocable outcomes.

The SIF and MOSAIC allow events, weighted for relevance, to be more readily visualized. MOSAIC delivers maps of data-driven and precise analytic conclusions containing both threat analytics and threat depiction. By using a systems science approach, we can see patterns that are only apparent when data are aggregated and analyzed with respect to their relevance to the ecosystems, communities, and technologies in which they occur. This allows us to build better scenarios from which we are better able to answer the real questions decision

makers have: what is the threat, where is it, and what kinds of activity are involved? Being able to leverage data-driven scenarios allows us to run through different types of responses regarding what are we going to do about it now, and in the future?

When it comes to the Arctic, these questions are less easily answered—not because we lack the technologies to do so but because our narratives about the Arctic are outdated and focused on geopolitical dynamics that miss the details of ACME. Compounding this is the tendency to review “security” in the Arctic through the lenses of politics, international affairs, and philosophy.

The initial assessment of asymmetric competition in the North American Arctic presented here is a snapshot that allowed the data to drive interpretation. The SIF and MOSAIC are not commodities for sale to the USG but rather a social ecological and technological systems science approach. From this snapshot, we derived three basic scenarios based on the best, most likely, and worst-case data products:

Scenario 1. Benevolent Overlord

AC winners, through a wide range of outreach, engagement, and support, establish relationships with a range of entities and institutions. The main focus is on shared goals toward ensuring resilience and sustainability under conditions of rapid and undesirable environmental and climate change. Engagements across academia and, in particular, nongovernmental groups such as think tanks, ensure that any perceptions of the PRC as a threat actor are softened through personal and professional collaborations. Over time, reliance and acceptance reach a threshold of comfort where subtly shifting values and practices are viewed as benign and, ultimately, desirable. No conflict is necessary and the co-opting of democratic ways of life is subtle and slow. Values are communicated through a range of outlets to include television, movies, investments in education, cultural exchanges, and support for local ways of life. Many of these values are, indeed, shared, such as those of strong and resilient communities. The veil of communism and control becomes so thin that it is no longer perceived.

Scenario 2. Resource Master

AC winners can acquire a remarkable range of assets at all scales, particularly those that fall beneath requirements of review (e.g., the Committee on Foreign Investment in the United States) and those that bring tangible benefits to the communities in which they occur, such as jobs or amenities that improve quality of life. Eventually, a robust enough portfolio of acquisitions results in an extensive set of constellation

information. In other words, the AC winner ends up with the better and greater knowledge to leverage natural resources, possess the logistics to exploit them faster, and develop the markets that do not require the United States to be a buyer.

Scenario 3. Kill Switch

AC winners have acquired enough tangible control (e.g., information, resources, and infrastructure) as well as co-optation of citizens, who do not perceive a threat. Such winners have acquired better scientific understanding so as to possess levers of ultimate control: the kill switch. Such levers range from the ability to limit communications or supply chains to the means to prevent the defense assets of the target nations and their allies from mobilizing and/or being effective. The Kill Switch scenario is the Black Swan—a set of events whose probability of occurring is extremely low but whose consequences would be devastating.

These scenarios provide a tangible basis for collectively developing approaches to policy and planning for Arctic security and defense in the context of asymmetric competition—responding to the recent calls for “thoughtfully executing, evaluating, and improving the nation’s Arctic security strategies.”³⁷

Conclusions

The scale of adversarial activities within the United States and Canadian Arctic, a region of growing geostrategic importance, far outpaces the existing narrative of the Arctic as a defense backwater. While not presented in this article, our data also indicate similar patterns across other Arctic nations. These activities in the Canadian and US Arctic are being conducted in the open at the seams of our institutional authorities, awareness, and response threshold. Perhaps the most challenging issue is that the free and open nature of our liberal democracies provides competing powers like the PRC and Russia with scientific, cultural, sociological, and other information sets that would have been unthinkable during the Cold War. This vastly increases the adversaries’ options in areas such as influence campaigns, space-based communications, airborne offensive systems, and subsurface warfare, while limiting those of the United States and its allies. As our option sets become reduced, the very technologies we are targeting to enable defense and security assets may become maladaptive. In other words, because we lack the best available knowledge in the Arctic regarding AC activities and their consequences, we may literally be playing into a technology trap where our investments today have little effect in the future because national intelligence analysis about the Arctic is flawed and our scenarios misinformed.

We spend a disproportionate amount time, energy and money constructing narratives that “threats are emerging in the Arctic.” We spend considerably less

time applying systems science to (1) precisely formulate them, (2) build data-driven scenarios, and (3) enact true joint, interagency, intergovernmental, and multinational strategies to accomplish 1 and 2.

Based on the scenarios offered above, we recommend the following actions to quickly update our approaches to responding to Arctic asymmetric competition.

Recommendation 1: Include the Arctic as part of the Indo-Pacific. For far too long the Arctic security and defense communities have remained static in their narratives and analyses. By recognizing that the Arctic is global in its biophysical and strategic influence, we will not only more readily detect patterns but also be able to apply them to other regions.

Recommendation 2: Leverage the Ted Stevens Center for Arctic Security Studies as the next-generation venue for Arctic analyses and narratives that more accurately depict security threats in an era of asymmetric competition. The Stevens Center is an opportunity to truly understand the Arctic as well as educate, train, and build collaborations across Arctic operators and practitioners.

Recommendation 3: Establish Arctic Technical Requirements for Irregular Warfare and Asymmetric Competition by looking to the United States Special Operations Command and its expertise in the tactics, techniques and procedures inherent in AC. While technical requirements currently exist for conventional warfare, none exist that can effectively guide integrated deterrence. By doing this with international partners, for example, through NATO's Multinational Capabilities Development Campaign (MCDC), we can strengthen alliances.

To date, the PRC has obtained access to tangible resources, a wealth of geophysical, sociocultural, linguistic and biophysical information about the Arctic. Their multilayered access to competing sovereign claims and conflicting jurisdictions and strategic postures offers a range of options to equip them for success in the future. The knowledge the PRC has gained over the past 15 years, and Beijing's clear efforts to expand its Arctic presence show that China is pursuing—and may in fact have—the expertise required to expand its options in the region while limiting those of the United States and its allies. It will take an integrated approach across all federal agencies, not just the DOD, and new, innovative partnerships, particularly with academia, to develop and apply an effective set of responses to ensure US Arctic security. ★

Dr. Lillian “Doc” Alessa

Doc Alessa is serving on an Intergovernmental Personnel Act with US Special Operations Command. She is a President's Professor at the University of Idaho and Director of the Center for Resilient Communities (CRC) and has published more than 150 peer-reviewed papers on systems science. She has previously served as a Defense Intelligence Senior Level (DISL)-equivalent Special Advisor to the Department of Defense (DOD) and was Deputy Chief of Global Strategies with the Department of Homeland Security (DHS), Office of Strategy, Policy, and Plans.

She has more than 25 years of Arctic experience working with academic, federal, state, local, tribal, and territorial partners across Canada and the United States focused on the resilience of systems, people, and communities. An internationally recognized expert in Arctic resilience, early warning systems, and special operations, she has led the development of the joint Canada–US Arctic resilience toolbox assessments: The Arctic Water Resources Vulnerability Index (AWRVI), the Arctic Adaptation Exchange Portal (AAEP), and the Permafrost Vulnerability Index (PVI). She has served on the Board of Directors for the Arctic Research Consortium of the US (ARCUS) and is a member of the National Academies of Science, Engineering, and Mathematics' Committee on Leveraging the Future Research and Development Landscape for the Intelligence Community. Doc Alessa is an author for the 5th *National Climate Assessment* and the US lead for the NATO Multinational Capabilities Development Campaign Climate Security Working Group.

CDR James Valentine, USCG, Ret.

Mr. Valentine is a retired United States Coast Guard (USCG) Commander (O-5/NATO OF-4) with two decades of intelligence experience. While on active military duty he served in intelligence billets ranging from field to national policy positions. In his final assignment from 2017-2019, he was a Senior Adviser to the United States Council on Transnational Organized Crime, serving six cabinet officers under Executive Order 13773. Over his career he received several personal awards, including the National Intelligence Superior Service Medal (NISSM) from the Director of National Intelligence, in 2016. He is now a research associate with University of Idaho's Center for Resilient Communities (CRC), while pursuing a master's degree in geoinformatics and geospatial intelligence at George Mason University. He has an MS in strategic intelligence from the National Intelligence University in Washington, DC (2005), and a BS in government from the United States Coast Guard Academy (1997).

CDR Sean Moon, USCG, Ret.

Mr. Moon is the Chief of Global Strategies in the US Department of Homeland Security Office of Strategy, Policy, and Plans, Washington, DC. He is currently seconded to the Department of Defense in support of Arctic strategic issues. Between 2011 and 2016, he served the DHS as the Director, Transportation and Cargo Policy and chaired the Asia-Pacific Economic Cooperation Sub-group for Maritime Security. A 1985 graduate of Willamette University in Salem, Oregon, he spent four years in the private sector before joining the US Coast Guard in 1989. Over the course of a 20-year career, he served as a Marine Safety officer, specializing in port operations and emergency management, community engagement, commercial and passenger vessel and facility safety and security programs. Mr. Moon has led strategic development and coordinated security issues across DHS, the interagency, and internationally since 2006.

Dr. Andrew Kliskey

Dr. Kliskey is President's Professor of Community & Landscape Resilience and the Director of the University of Idaho Center for Resilient Communities (CRC). Kliskey is also the Idaho EPSCoR Director (Established Program to Stimulate Competitive Research). He is a social-ecological systems scientist and behavioral geographer with training, teaching, and research experience in landscape ecology, behavioral and perceptual geography, geographic information systems (GIS), planning, policy analysis, and surveying. Andy has spent the past 20 years working in Maori communities in New Zealand, rural communities in western Canada, Inupiat communities in northwestern Alaska, Denai'na communities in southcentral Alaska, and rural communities in Idaho, examining community and landscape resilience. His teaching and research are interdisciplinary in nature and directed at integrated methodologies in social-ecological systems that combines stakeholder-engagement, scenario analysis, and geospatial modeling. Kliskey is project lead on two National Science Foundation Innovations at the Nexus of Food, Energy, and Water Systems (INFEWS) awards.

Notes

1. Matthew Kroenig, *The Return of Great Power Rivalry : Democracy Versus Autocracy from the Ancient World to the U.S. and China* (New York: Oxford University Press, 2020); Walter Russell Mead, "The Return of Geopolitics: The Revenge of the Revisionist Powers," *Foreign Affairs* 93, no. 3 (2014): 69–79; and Antulio J. Echevarria II, *Operating in the Gray Zone: An Alternative Paradigm for U.S. Military Strategy* (Carlisle Barracks, PA: US Army War College Press, April 2016), <https://press.armywarcollege.edu/>.
2. George Kennan, "Policy Planning Staff Memo 269," US Department of State, Office of the Historian, 5 April 1948, <https://history.state.gov/>.
3. United Nations, "Universal Declaration of Human Rights," 10 December 1948, <https://www.un.org/>.
4. NATO, "The North Atlantic Treaty," 4 April 1949, <http://www.nato.int/>; and The International Criminal Court, "The ICC at a Glance," 2019, <https://www.icc-cpi.int/>.
5. Karl E. Nell, "A Doctrine of Contingent Sovereignty," *Orbis* 62, no. 2 (2018): 313–34, <https://www.sciencedirect.com/>; and Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* (Princeton, NJ: Princeton University Press, 1999).
6. Joanne Smith Finley, "Why Scholars and Activists Increasingly Fear a Uyghur Genocide in Xinjiang," *Journal of Genocide Research* 23, no. 3 (July 2021): 348–70, doi: 10.1080/14623528.2020.1848109; and Donald C. Clarke, "Hong Kong's National Security Law: a first look," *The China Collection*, 30 June 2020, <https://thechinacollection.org/>.
7. Kennan, "Policy Planning Staff Memo 269."
8. "Communiqué on the Current State of the Ideological Sphere," as quoted in Chris Buckley, "China Takes Aim at Western Ideas," *New York Times*, 19 August 2013, <https://www.nytimes.com/>.
9. Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, 1999).
10. Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats, "Hybrid threats as a concept," n.d., <https://www.hybridcoe.fi/>.
11. Echevarria II, *Operating in the Gray Zone*; and Jill I. Goldenziel, "Law as a Battlefield: The U.S., China, and Global Escalation of Lawfare," *Cornell Law Review* 106 (25 January 2020): 1085–171, <https://ssrn.com/>.
12. Hybrid CoE, "Hybrid threats as a concept."
13. Omer Dostri, "The Reemergence of Gray-Zone Warfare in Modern Conflicts Israel's Struggle against Hamas's Indirect Approach," *Military Review* 100, no. 1 (2020): 120–27.
14. Frank Watanabe, "How to Succeed in the DI: Fifteen Axioms for Intelligence Analysts (U)," Central Intelligence Agency CSI Publication, 1997, 3; and Lauren Witlin, "Mirror-Imaging and Its Dangers," *SAIS Review of International Affairs* 28, no. 1 (2008): 89–90.
15. Watanabe, "How to Succeed in the DI."
16. John G. Heidenrich, "The State of Strategic Intelligence — Central Intelligence Agency," *Studies in Intelligence* 51, no. 2 (2007): 15–26.
17. United States Department of Defense, Report to Congress: Department of Defense Arctic Strategy, Congressional Report RefID: 0-5064821 (Washington, DC: US Department of Defense, May 2019).
18. Dylan Craig, *Sovereignty, War, and the Global State* (Cham: Palgrave-MacMillan, 2020), doi: 10.1007/978-3-030-19886-2; and Dylan Craig, "Intermediarized Security Governance and

the 'Sultans' Retort',” *Journal of the Middle East and Africa* 5, no. 2 (May 2014): 131–49, doi: 10.1080/21520844.2014.926248.

19. Mao Zedong, “The Collected Works of Mao Zedong Vol I: On Correcting Mistaken Ideas in the Party, December 1929,” Marxists Internet Archive, 2004, <https://www.marxists.org/>.

20. Information Office of the State Council, People’s Republic of China, “China’s Military Strategy (full text),” 27 May 2015, <http://english.www.gov.cn/>.

21. Conor M. Kennedy and Andrew S. Erickson, “China’s Uniformed, Navy-Trained Fishing ‘Militia’,” *The Maritime Executive*, 17 May 2016, <https://www.maritime-executive.com/>.

22. Center for Circumpolar Security Studies, “The Arctic Institute: Facts & Figures,” *The Arctic Institute*, 19 June 2020, <https://www.thearcticinstitute.org/>.

23. Patricia Zengerle, “China granted observer seat on Arctic governing council,” *Reuters*, 15 May 2013, <https://www.reuters.com/>.

24. Stephen Chen, “China launches overseas satellite ground station near North Pole,” *South China Morning Post*, 16 December 2016, <https://www.scmp.com/>.

25. Arctic Observatory, SES and Polar Research Institute of China, “China-Iceland Arctic Observatory,” 2018, <https://karholl.is/en/>.

26. Information Office of the State Council, People’s Republic of China, “China’s Arctic Policy: Full Text,” 26 January 2018, <http://english.www.gov.cn/>.

27. Gisela Greiger, “China’s Arctic policy: How China aligns rights and interests.” *European Parliamentary Research Service*, May 2018, <http://www.iberchina.org/>.

28. Greiger, “China’s Arctic policy.”

29. Greiger, “China’s Arctic policy.”

30. Heather J. Williams and Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise* (Santa Monica, CA: RAND Corporation, 2018), doi: 10.7249/RR1964.

31. Office of the Director of National Intelligence, “Intelligence Community Directive 203: Analytic Standards,” 2 January 2015, <https://www.dni.gov/>.

32. Boundary disputes, such as the Beaufort Sea boundary between the United States and Canada were immaterial when scoring and analyzing the aggregated events across the study area; the location is inside the maritime claims of both nations, satisfying the weighting criteria. If analyzing the data separately for the United States and Canada, then the logical choice would be to use the U.S. claims when analyzing the U.S. portion of the study area, and the Canadian claims for the Canadian analysis, as the threat would be relative to the nation examined. United Nations, “United Nations Convention on the Law of the Sea of 10 December 1982,” 10 December 1982, <https://www.un.org/>; Flanders Marine Institute (VLIZ), Belgium, “Maritime Boundaries Geodatabase,” 2019, doi: 10.14284/382; and “Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks,” *Ocean Yearbook Online*, 12, no. 1 (1996), 471–500, doi: 10.1163/221160096X00418.

33. Kenneth Ewart Boulding, *Conflict and Defense: a general theory* (New York: Harper & Row, 1962); and Waldo R. Tobler, “A Computer Movie Simulating Urban Growth in the Detroit Region,” *Economic Geography* 46, no. 1 supplemental (1970): 234–40, doi: 10.2307/143141.

34. George Kingsley Zipf, “The P1 P2/D Hypothesis: On the Intercity Movement of Persons,” *American Sociological Review* 11, no. 6 (December 1946): 677–86, doi: 10.2307/2087063; James E. Anderson, “The Gravity Model,” *Annual Review of Economics* 3, no. 1 (September 2011): 133–60,

doi: 10.1146/annurev-economics-111809-125114; and Jacques Poot, et al., “The gravity model of migration: the successful comeback of an ageing superstar in regional science,” IZA Discussion Paper No 10329, 2016, <https://papers.ssrn.com/>.

35. Haversine vice geodesic distance was chosen to speed calculation while maintaining acceptable error in the results (+/-0.03% distance error when compared to geodesic.)

36. National Research Council, *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences* (Washington, DC: The National Academies Press, 2011), doi: 10.17226/13040; and Artner Stephen, Richard S. Girven, James B. Bruce, *Assessing the value of structured analytic techniques in the US intelligence community* (Santa Monica, CA: RAND, 2016).

37. David Krumm and Matthew Nicholson, “The Arctic in an Age of Strategic Competition,” *Journal of Indo-Pacific Affairs* 4, no. 7 (October 2021): 26–35, <https://media.defense.gov/>.