THE INTERNATIONAL JOURNAL OF INTELLIGENCE, SECURITY, AND PUBLIC AFFAIRS
https://doi.org/10.1080/23800992.2021.2006954

Surprise and Suspense: How the Intelligence Community Forgot the Future

Lilian Alessa[a], Sean K Moon[b], James Valentine[a,c], Michael Hepburn[d], Don Kliskey[e], and Andrew [a]

[a]College of Art & Architecture, University of Idaho, USA; [b]Global Strategies, Office of Planning Policy and Strategy, Department of Homeland Security, , Washington, USA; [c]United States Coast Guard, Washington, District of Columbia, USA; [d]National Center for Autonomous Technologies, USA; [e]Boanerges Solutions, USA

ABSTRACT

This paper examines the challenges faced by the U.S. intelligence community (IC) in recognizing and responding to the elements inherent in asymmetric competition with China. We offer that cultural and procedural impediments are negatively impacting the community's capabilities and argue that reliance on outdated methodologies and ad hoc technology acquisition to detect activities specific to asymmetric competition has allowed adversaries to exploit three types of interstitial gray areas (IGA) – operational, organizational, and informational. We argue that an updated framework to combat emerging threats from asymmetric competition and commensurate IGAs that has been proven in field settings to enhance detection, deterrence, denial, diplomacy, and defense against adversarial actions is needed. We demonstrate how the framework improves security resilience by focusing more on the human as a driver and user throughout the system, enabled by technological tools that start with the development of more diverse rules for data analytics through inputs from of federal, state, local, territorial, tribal, provincial, and private sector operators.

ARTICLE HISTORY
Received 18 May 2020
Revised 16 April 2021
Accepted 9 November 2021

KEYWORDS
Asymmetric competition; Data analytics; irregular warfare; national security; strategic intelligence framework

1. Introduction

Over the years the term "Great Power Competition" (GPC) has come and gone and means many things to different people. We use the term "asymmetric competition„ instead and define this as the tension between the specific will of a given nation state exerted on the international system structure through activities, both licit and illicit, which in aggregate, are incompatible with the desires of another nation state. It may be further defined as involving two or more nation states strong enough to change the system of world order through an aggregate of activities imposed both within and outside their borders. Ultimately, no matter what it is called the elements within asymmetric competition will remain a significant challenge to the US Intelligence Community (IC), both domestically and globally.

CONTACT Andrew Kliskey akliskey@uidaho.edu Center for Resilient Communities, University of Idaho

Table 1. A comparison of the United States' 2017 National Security Strategy with the 2020 National Counterintelligence Strategy and the 2018 National Defense Strategy.

			National Counterintelligence Strategy of the United States of America 2020–2022					2018 National Defense Strategy of the United States of America		
			Objective 1	Objective 2	Objective 3	Objective 4	Objective 5	Line of Effort 1	Line of Effort 2	Line of Effort 3
			Protect the Nation's Critical Infrastructure.	Reduce Threats to Key U.S. Supply Chains.	Counter the Exploitation of the U.S. Economy.	Defend American Democracy against Foreign Influence.	Counter Foreign Intelligence Cyber and Technical Operations.	Build a Lethal Force.	Strengthen Alliances.	Reform the DoD Department.
2017 National Security Strategy of the United States of America	Pillar I	Protect the American People, the Homeland, and the American Way of Life.	✓	✓	✓	✓	✓	✓	✓	✓
	Pillar II	Promote American Prosperity.	✓	✓	✓	✓			✓	
	Pillar III	Preserve Peace through Strength.	✓	✓	✓	✓	✓	✓	✓	✓
	Pillar IV	Advance American Influence.	✓		✓	✓		✓	✓	✓

The U.S. IC has a lengthy history of failing to identify or predict significant events, resulting in the United States being strategically surprised. Between 1950 and 2020 there were at least 28 large-scale events that the IC failed to recognize or forecast, ranging from the invasion of South Korea by North Korea to the Arab Spring and the recent Russian hacking of U.S. government agencies (Figure 1). As recently as August, 2021, the IC was surprised when China demonstrated an advanced space-capable hypersonic missile. While hypersonic weapons development was already a topic of interest to the IC, it missed the advanced state of development and that China's weapon was orbital-capable (Shoaib, 2021). Even though the IC may have detected and prevented other events, this average failure rate of once every 2.5 years, and the scale of the events missed, is significant. And it has occurred even while the United States has made enormous investments in intelligence technologies, personnel, and strategies (Table 1). Just between 2001 and 2012, intelligence appropriations roughly doubled, to at least $78 billion, a figure almost twice as large as during the Cold War (Erwin & Belasco, 2013). The IC has also been reformed multiple times over the course of its history, often as a result of significant failures and in an attempt to prevent future deficiencies (Federation of American Scientists, 2021; ODNI, 2021)

Recently, the domestic elemnts of the U.S. IC, particularly its Law Enforcement components, failed once again when on January 6, 2021, an armed insurrection took place in the U.S. Capital Building. Thousands stormed the joint session of Congress in a deadly effort to disrupt counting

Figure 1. Strategic surprises experienced by the United States and the U.S. Intelligence Community, 1950 to 2020 (Aid, 2011; Dilinian, 2012; Everett & Gerstein, 2014; Fruhlinger, 2020; Glasser, 2017Hedley, 2005; Krepon, 2008; Ochiai, 2011; The 9/11 Commission, 2004).

of Electoral College votes and certification of the new President-elect (Barrett & Zapotosky, 2021). Analysis of the incident indicates that the Departments of Homeland Security and Justice were unable to provide adequate intelligence and threat assessments to law enforcement partners, despite significant pre-existing intelligence collections that were available for analysis and might have provided alerts and warnings (Margolin & Bruggeman, 2021). The Federal Bureau of Investigation (FBI) had adequate warning from its Norfolk Field Office, which was transmitted to FBI Headquarters, but it was not considered "finally evaluated intelligence," and any agencies receiving it were requested not to act without prior coordination with the Bureau (Barrett & Zapotosky, 2021). Given this history of failure, the choice before us is adapt to reality or fail.

1.1 Methodology

In response to repeated calls from across the U.S. Government (USG) we spent the past four years using the Quadrant Enabled Delphi (QED) method (Alessa, Moon, Griffith, & Kliskey, 2018a) to work with a coalition of the willing within law enforcement, policy, intelligence, and defense community practitioners to assess risk environments, potential mitigation actions, and impediments to effective security for the United States and Canada.

The original Delphi method was developed in the early 1950s by Olaf Helmer and Norman Dalkey to systematically solicit the view of experts related to national defense and later adapted for use in other areas of socio-political discourse. The term originates from Greek mythology: Delphi was the site of the Delphic oracle, the most important oracle in the classical Greek world. Thus, the Delphi method may be thought of as expert brainstorming (Adomavicius & Tuzhilin, 2005).

QED is a rapid, in-person method of eliciting, discussing, organizing, and prioritizing information directly from operators, unit level personnel, or any group of subject matter experts. Based on cognitive science and human organization principles, the method values each individual as a database of tacit and implicit knowledge based on real-world experience and proficiency (Custer, Scarcella, & Stewart, 1999; Scheele, 1975). The outcomes of the method are a) a concise set of priorities for any given issue such as threats, b) capability or functional gaps that need to be addressed and c) possible means to address them. QED workshops are typically 1 to 2 days in duration, depending on the topic, and can involve up to 100 participants (though 25 to 40 are ideal) and meta-analysis is performed across different QEDs.

QED enhances the precision and effectiveness of decision-making in larger groups across a range of topic areas utilizing Delphi Method concepts in combination with the Nominal Group Technique/Pareto N3 Dot Exercise (Alessa et al., 2018a; Paul, 2008; Schmidt, Lyytinen, Keil, & Cule, 2001).

QED replaces traditional Delphi pre-workshop surveys with recursive, in-person social processes: experts are brought together, and elicitation of expert knowledge and consensus-building occurs through facilitated group sessions with iteration and refinement occurring through a series of structured sessions.

In QED, facilitators initially present a series of carefully crafted challenge questions to a diverse group (the Delphi group) to initiate discussion. These questions are specific to the topic at hand but crafted so as not to introduce bias. Facilitators then oversee responses of the panel of experts, helping them express their opinions concisely and accurately while recording the points raised. The meeting venue is divided into quadrants based on broad topic areas (e.g., 'maritime' or 'cyber') related to the overall workshop topic. Participants are not seated by quadrant, but rather interact with all quadrants. Additionally, during many exercises (i.e., the Pareto Dot exercise), participants move amongst the quadrants, interactively. A facilitator (or "quadrant manager") familiar with the quadrant topic is assigned for each quadrant. The central facilitator (or "room manager") coordinates the overall discussion and roams among the different quadrants. Each quadrant facilitator engages the participants in their quadrant through verbal, visual, and physical cues. Quadrant facilitators also liaise with the central facilitator to adjust information elicitation based on the agent types in their quadrant (Alessa & Kliskey, 2012).

QED also recognizes the communications styles of differing personality types. For instance, more introverted people may tend to prefer written communications. To ensure that input from all participants is elicited impartially, participants are also encouraged to offer written observations by way of an anonymous drop box. Written observations are collated by facilitators and presented to the Delphi group as part of the overall facilitator interaction process, in order to foster cognitive cascades. Maps, charts, and other visual aids are also used to gather and disseminate data.

In a series of QED workshops on topics ranging from data integration and information sharing to all domain intelligence requirements, 474 Federal, State, Local, Tribal, Territorial, Provincial, and Private Sector (FSLTTPP) law enforcement, policy, intelligence, and defense community practitioners provided insights that led us to identify three types of Interstitial Gray Areas (IGAs); Operational, Organizational, and Information (Data and Analytics) (Votel et al., 2016). In order to address those IGAs, and based upon insights garnered from the workshops, our studies resulted in the creation of a mission-agnostic, USG-substantiated and operator-driven Strategic Intelligence Framework (SIF) as a guiding set of activities adapted to better detect asymmetric competition activity patterns hidden within noise.

The SIF utilizes the end-to-end assets of human knowledge, diverse data ecosystems and mathematical/computational tools, such as artificial intelligence and machine learning to accelerate all-domain awareness and identify collection gaps. This framework overcomes the dangers associated with attempts to establish a standardized digital foundation which could put our intelligence enterprise at risk due to losing the very data which reflect asymmetric competition activities.

The outputs of the SIF are visualized through the *Mesoscale Operational Situational Awareness Intelligence Composite* (MOSAIC) which allows operators to readily make sense of signals hidden in the noise for actionable intelligence that is both timely and credible (Figure 3). The SIF accommodates the complexity of the new and ever-changing asymmetric competition threat landscape by enabling a science of security (Alessa, Moon, & Valentine, Forthcoming), with humans as *rule managers at the core, using robust social-ecological, complex adaptive systems principles and artificial intelligence/machine learning (AI/ML) as augmentation to accelerate analysis*. This end-to-end integration of human cognitive strengths with artificial intelligence and machine learning enables us to get precise answers to difficult questions necessary to acquire and excel in maintaining strategic advantages across the IC and Law Enforcement (LE) continuum.

As a proof of concept, the SIF was applied toward asymmetric competition activities in the U.S. Arctic using open-source information (Alessa et al, Forthcoming). For the purposes of this exercise, QED workshop participants were treated as Rule Managers. Application revealed a pattern of activities that most closely resemble irregular warfare and operational preparation of the environment (IW/OPE).[1] Here, IW refers to adversarial activity, both overt and covert, which is not conventional or regular, that is, 'war by any means' to include information campaigns, collections efforts whether organized or opportunistic. Such activities are targeted at general interruptions, interference and immersion in all aspects of the functioning of a society, it's patterns of life (POL) and capabilities for security and defense. OPE refers to activities that prepare the way for overt military action, including softening a populace, preparing them for nonstandard social norms, and can turn previously loyal citizens against their own governing bodies. Based on our on-going analysis this pattern has been in place for at least two decades and was missed in aggregate by the IC. We note that this failing is repeated across the world and has been exacerbated by the COVID-19 pandemic, which has denied a significant proportion of the IC access to their classified systems, though the duration of the crisis has allowed elements of the IC to adapt (USGIF, 2020). Due to a historic reliance on overclassification and ingests via these systems, the pace of potential adaptation by the IC has been slowed even further, placing the United States on an even more unstable footing going into an uncertain future (Young, 2019). This at a time when China has presented a stronger stance, including exerting influence within

academia, conducting cyber activities such as hacking and social media influence campaigns, as well as more traditional espionage activities, for an extended period of time (Mattis, 2015; Tatlow, 2020; USCC, 2016, 2020).

1.2 QED workshops – Selected overviews

February 1–2, 2017 – Emerging Arctic Security Threats Matrix (EARTh-X) for Improved Canada-United States (CANUS) Arctic Security (Alessa, Moon, Griffith, Kliskey, & Bielby, 2017a)

EARTh-X was the first foundational study of the Arctic Homeland Security (vice National Defense) risk environment. Participants enumerated 198 threats in the Arctic Security sector. Fourteen threats were ranked as highest in severity using the Nominal Group/Pareto Dot method. After narrowing the list to the "most serious" threats from the Maritime, Air, Cyber, Land, or Other/All security domains, participants ranked them in terms of overall Priority (the order in which threats should be addressed given limited available resources, from highest to lowest). The participants also assigned estimates of Time Scale (immediacy of threat) and Spatial Scale (local, national, or international scope) to each threat.

February 23, 2017 – Northern Border Security Review (NBSRA) (Alessa, Moon, Griffith, Kliskey, & Bielby, 2017b)

Participants enumerated 89 Northern Border threats across five categories – maritime, air, land, cyber, and "other" (encompassing threats not readily categorized). Additional written input, voluntarily submitted via an anonymous comment box, added significant details about specific threats. The threat list was narrowed to the "most serious" threats from each security domain and the lists were ranked by participants in terms of overall priority (the order in which threats should be addressed given limited available resources, from highest to lowest). The participants also ranked the priorities based on immediacy of threat (time scale) and whether they were local, regional, or national in scope. The greatest eight threats were identified using the Nominal Group/Pareto Dot method.

*June 13–14, 2017 – Port of San Diego Vulnerability Assessment (PVA) (*Alessa, Moon, Griffith, & Kliskey, 2017c)

The Port of San Diego (POSD) hosted a Port Vulnerability Assessment (PVA) to better understand threats and vulnerabilities associated with critical infrastructure in the Port. Security experts with domain and local expertise attended and were representative of private and public concerns in the POSD. Threats were discussed as Critical Cascade Points (C2P) to highlight areas and equipment where a failure or attack would cause cascading negative effects in other Port components or the larger transportation system. The assembled port security domain experts collectively enumerated 88 threats in or around

the POSD during QED sessions, and participants provided additional written comments on specific threats. To produce an initial Threats Matrix, the enumerated threats were ranked based on severity and time scale.

November 9, 2017 – Central America Pacific Rim Risk Intersections (CAPRRI) (Alessa, Moon, & Bielby, 2017d)

CAPRRI was originally focused on better understanding the risk intersections inherent in Central America and the Pacific Rim (including Alaska and the Arctic). Shortly into the workshop it became obvious that there exist key impediments preventing our ability, as a whole of government effort, to do such an assessment: A lack of data diversity, poor information sharing across agencies focused on shared/resonant missions sets (e.g., Countering Transnational Organized Crime), and poor coordination and information/data sharing across FSLTTPP partnerships, in part due to over-classification of data but also due to a growing "silo-syndrome" of decreasing communication outside cliques. While CAPRRI was able to identify risk intersections, a significant portion of the exercise was re-focused on exploring these impediments.

March 10, 2018 – Data Integration and Information Sharing (DIIS) (Alessa, Moon, Griffith, Kliskey, & Bielby, 2018b)

DIIS followed on to CAPRRI, focusing on expanding understanding of the impediments to using data, information, and intelligence and potential mitigations to those barriers. Initial group elicitation identified the status quo and capability gaps. The Pareto Dot exercise refined and prioritized the identified status quo and capability gaps. Data analysis was conducted using weighted linear regression through the modified Pareto process. 1,367 data points were collected over two days, and 181 narratives were collected from participants to expand on the data points.

April 10, 2018Improved Data Access/Fusion/Sharing for Joint Task Forces (JTF-RAPID) (Alessa & Moon, 2018c)

JTF-RAPID focused on impediments to success within the DHS JTF construction, addressing disconnects between the DHS Joint Analysis Group (DJAG), establishing the DHS Data Framework, the Joint Task Forces (JTF), and the broader synergies across the federal inter-agency.

August 15–17, 2018 Coastal Observing and Data/Information Sharing for Security (CODISS) (Alessa, Moon, Griffith, & Kliskey, 2018d)

CODISS addressed rapidly changing maritime environments and the adversaries that operate within them affecting several aspects of nearshore littoral and landward systems that: a) alter ecologies which destabilize local communities, b) allow the intrusion of threat actors ranging from Nation State actors to transnational criminal organizations, and c) challenge our abilities to adapt quickly enough to mount effective responses that ensure the security and safety of the Homeland. CODISS was held to survey the assets and capabilities in maritime surveillance and determine critical gaps and potential means of

closing them. It focused on observing networks and the sensors therein (ranging from satellite to radars to humans) used for a range of purposes: e.g., to help guide economic development (e.g., aquaculture, fisheries, and tourism), law enforcement, community resilience and infrastructure integrity (Alessa et al., 2016).

April/May 2020 – COVID-19 Agricultural Economic Security Response, Prevention, Mitigation Scenarios

Shortly after COVID-19 pandemic began, the DHS Cyber and Infrastructure Security Agency (CISA) identified a need for a forecasting tool to support their then-new Futures Look cell. A suite of algorithms was developed to ingest data from a wide swatch of sources, identify current trends, and establish impacts on those trends based on future forecast conditions (e.g., active Hurricane season, extensive wildfires/droughts, etc.). The analytics are available at:

https://storymaps.arcgis.com/stories/1ca1ae7afe374fd4a30689e684b50867.

June 2–3, 2020 – Arctic Trix (Alessa & Moon, 2020)

The Arctic Trix workshop provided a forum for participants ranging from operators to senior officials and flag officers to discuss the variables of concern (those that "keep them up at night") in the context of Arctic security and defense specific to near-peer competition by the Russian Federation (RF) and People's Republic of China (PRC). Participants' input further contributed to an on-going assessment of the Arctic with an emphasis on Canada's and the United States' strategic interests therein (Office of the White House, 2013). They were asked to consider a range of variables specific to events which could abruptly threaten the North American homelands. A primary objective was to elicit the science/rationale/evidence behind why these particular activities, issues, dynamics, or trends rose to the level of concern. Superimposed on broader considerations were the variable rates and types of adaptations to the COVID-19 pandemic. The workshop illuminated areas of concern that could be addressed in the next few months to a year (near term) out to five years (long term).

1.3 Problem context

The goal of acquiring and sharing intelligence is to gain a strategic advantage over an adversary to avoid surprise (ODNI, 2019). Implicit in this is an exquisite awareness of changes in a staggering array of variables constantly in play at any given time. The scope of this paper is not to display the range of failures of the intelligence community, which have been extensively discussed in a range of publications (Ucko & Marks, 2018) but rather to provide some suggestions to the IC to adapt more quickly to the threat landscape so as to avoid surprise. We define surprise in the scientific terms of complex adaptive systems whereby global minima in data and information (e.g., activities that do

not rise above reporting thresholds) are missed in analysis (e.g., lacking a framework to aggregate key activities in space and time) resulting in the eruption of a new global maxima in the form of activities (e.g., COVID-19) for which we had little or no early warning and are thus unprepared.

Why is this? In a nutshell, it is because we use old methods and target the wrong data using processes based on the dated philosophies of Sherman Kent, considered by some to be a founding father of Allied intelligence analysis during World War II and the Cold War (Davis, 2002; Garten, 2019). While Kent's fundamental analytic doctrine remains sound (e.g., intelligence analysts are providers of information and insight for policy decisionmakers and action-takers), his vision of "an elevated debate" taking place among professionals with a deep understanding of world history and current events, standing on the foundation of a shared analytic process, is at best aspirational. Kent created an analytic framework that relies upon the professional acumen of highly trained and experienced analysts. The current information age, in which analysts are overwhelmed by classified and unclassified data, was never imagined (Young, 2019). Nor was an IC workforce that would become a large, cumbersome, poorly trained bureaucracy (Stimpson & Habeck, 2016; Vance, 2018). Nor did Kent foresee an intelligence enterprise in which authorities are stove-piped such that no holistic approach to national security exists (Kindsvater, 2008), and where barriers to information sharing between law enforcement and intelligence organizations degrade protection of the homeland (Grewe, 2004; Manrique, 2018). As a result, instead of analysis based on sound scientific principles, we rely upon a range of activities that are less effective and based upon opinion and stagnant traditions (Dunn-Cavelty & Mauer, 2009). Activities such as red teaming and net assessment, in which practitioners game potential scenarios, or geopolitical reports on nations of interest, particularly China, Russia, Iran, and North Korea, are based in large part on analyses that amount to little more than literature reviews, informed by collections driven by what analysts want to know, not what operators or policymakers need to understand (Hoover Institution, 2004; Stimpson & Habeck, 2016).

It is beyond the scope (and purpose) of this paper, and the subject of extensive other research, to dive deeply into the challenges faced by red teaming and net assessments. In precis, they are the result of both methodologies being reliant on the expertise and breadth of knowledge of the practitioners, which subjects them to cognitive biases and heuristics, as well as cultural resistance (Clark, Patt, & Walton, 2020; Marrewijk, 2018; Yanalitis, 2014). There are over 200 identified types of bias and/or heuristics potentially at play, each of which must be overcome with a successful mitigation strategy (Kardos & Dexter, 2017). Net assessment in particular is considered a practice, as opposed to an art or a science (Bracken, 2006). While it was seen as highly successful under the direction of its original and principal developer the

process required a thorough understanding of both our own and other nations' military capabilities, primarily those of the Soviet Union (Gertz, 2016). Absent this thorough understanding, net assessment lacks a quantitative objective core able to stand against the drift inherent in objective bias.

In addition to outdated processes, the IC relies on assessments of information and data that come in from a variety of sources ranging from human intelligence to satellite imagery which are often "analyzed" using black box technologies sold by the private sector to the USG (Margolis, 2013). Frequently, the only framework that is used is the observe-orient-decide-act (OODA) loop (Galinec & Macanga, 2012; Ling, Moon, & Kruzins, 2005), which in concept is sound but in practice has failed to adapt to the modern dynamic threat landscape. The OODA loop was developed before vast amounts of data were available on a minute-by-minute basis and when "intelligence products" could move at the pace of the technologies of the time. The world is faster now, and the IC still works at the pace of the past. Exacerbating this are narrow, stove-piped, or atrophied skills, reliance on outdated information models, and a philosophy that relies too heavily on disjunct commercial technologies to provide all-domain awareness in lieu of government off-the-shelf capabilities (Alessa et al., 2018a). As a consequence of this patchwork approach, the IC's indication and warning capability is all but comatose (Gentry & Gordon, 2019).

As was shown in Figure 1, the IC consistently misses patterns of sophisticated, highly coordinated acts designed to undermine our Nation's security and defense by exploiting the gaps and seams in our policies, processes, laws, authorities, and social frameworks. For example, the massive hacking of U.S. government and private sector computer systems in late 2020 involving malware attached to a software update from SolarWinds, currently attributed to Russia (Chappell, Myre, & Wamsley, 2020). Or the terrorist attacks of September 11, 2001 (The 9/11 Commission, 2004). As mentioned earlier, we refer to these spaces as Interstitial Gray Areas (IGAs) wherein licit, but nefarious, and/or illicit activities may remain undetected, falling outside our intelligence awareness, laws, policies, and authorities (Votel et al., 2016). This concept is not novel – it is a cornerstone of irregular warfare (IW) doctrine across the globe (Kiras, 2016; Ucko & Marks, 2018).

We now find ourselves in a weakened domestic and global position, not of our choosing, designed to defeat us without classic military action and occurring faster than we can counter (Dobbins et al., 2017; Dupont, 2020).

1.4 Responding to national strategies

Two key passages from the 2017 *National Security Strategy of the United States of America (NSS)* (Office of the White House, 2017) underscore the need for an integrated approach, in which counterintelligence, national defense, and national security are able to identify antagonist activities by harnessing data and using it in new ways to serve our collective National interests (Table 1).

> . . . many actors have become skilled at operating below the threshold of military conflict —challenging the United States, our allies, and our partners with hostile actions cloaked in deniability.
>
> The ability to harness the power of data is fundamental to the continuing growth of America's economy, prevailing against hostile ideologies, and building and deploying the most effective military in the world.

A comparison of the pillars of the NSS with the Objectives of the *National Counterintelligence Strategy of the United States of America 2020–2020* (Office of the Director of National Intelligence (ODNI), 2020) and the lines of effort of the 2018 *National Defense Strategy of the United States of America* (Odom, 2001; Office of the White House, 2018); Office of the White House's enterprise adaptation and illumination of currently hidden adversarial activities.

The IC itself identifies indication and warning as a central function. In the wake of September 11, 2001, it has rebranded this capability as "anticipatory intelligence," and transferred it away from specialized, highly trained personnel and into everyday analysis functions seriously eroding warning capability (Gentry & Gordon, 2019). Nevertheless, the *National Intelligence Strategy of the United States of America 2019* (ODNI, 2019) cites anticipatory intelligence as one of three foundational missions and directs that the IC will:

The theme was carried forward in the March, 2021 Interim National Security Strategic Guidance issued by the White House (Office of the White House, 20212021), in which the new Administration spoke to reinvigorating partnerships, using diplomacy before military, and ensuring the U.S. Armed Forces remain the best trained and equipped in the world.

"*. . . In the face of strategic challenges from an increasingly assertive China and destabilizing Russia, we will assess the appropriate structure, capabilities, and sizing of the force, and, working with the Congress, shift our emphasis from unneeded legacy platforms and weapons systems to free up resources for investments in the cutting-edge technologies and capabilities that will determine our military and national security advantage in the future.*"

> ". . . expand its use of quantitative analytic methods while reinforcing qualitative methods, especially those that encourage new perspectives and challenge long-standing assumptions."

2. Interstitial Gray Areas (IGAs) – Where Surprise is born

IGAs are identified in the defense literature that deals primarily with special operations in foreign theaters (Lohaus, 2015). Leveraging this knowledge and applying it to the homeland security/defense mission space we identify three types of IGA: Operational, Organizational, and Information (data and analytics).

2.1 Operational

Operational IGAs are tangible physical spaces in which adversaries and threat actors operate (Kiras, 2016). The expansive geography of specific regions of the United States and Canada means that operations are expensive at scale. Agencies such as the Department of Homeland Security (DHS), Department of Justice (DOJ), and Department of Defense (DOD) must therefore look beyond centralized "campaign-style" operations for success (DHS, 2014: DOJ, 2018). Current monitoring and observation systems (i.e., government and commercial satellites and ground-, air-, and maritime-based sensors) do not possess enough diversity nor do they have the resolution needed to combat adversaries *in situ* (Helal & Hassan, 2017). This over-reliance on large, commercial or government systems means that critical information and context to geospatial imagery is frequently not available, let alone in a timely manner, to FSLTTPP partners who can act. Systems that were built to be overtly focused on early warning for conventional defense lack the ability to identify activity that is literally "below the radar." The lack of a cohesive domestic counter-intelligence plan that spans the FSLTTPP spectrum has allowed adversaries to adopt an angle of attack consistent with irregular warfare: they will not expend effort where our defenses and security are strongest but rather exploit paths and avenues where we are not looking or are unable to see them (Tingstad et al., 2018). Even in regions where our technologies allow us to see almost everything, we lack a systematic means of acquiring context, emphasizing the tradecrafts such as networked human intelligence we have lost (Margolis, 2013). A more wicked problem stems from the unsurprising de-sensitization of the law enforcement community to noisy (aka "nuisance") events. These one-offs are often dismissed as "weird" or odd and may mimic an action/incident that is fully explainable. Given the immense workloads and declining resources allocated to law enforcement this is not unexpected, particularly if, as a savvy adversary would, analysis is done through POL to detect vulnerabilities in our homeland security and law enforcement enterprise.

Over-spending on off-the-shelf "solutions" has eroded the traditional human intelligence (HUMINT) tradecraft that is at the core of denying and defending against asymmetric competition activities on domestic soil. To truly enter the new threat landscape from a superior stance, we must

reclaim the science and skills of an integrated and sophisticated HUMINT enterprise. It is important to recognize that the use of informant, especially criminal informant/source networks, remains robust, but we have not taken advantage of the science of informative networks which differ significantly (Alessa & Kliskey, 2012; Griffith, Alessa, & Kliskey, 2017; Hepburn, 2018). The latter add critical context and veracity on the ground that is not limited to a single mission, providing breadth across a suite of variables that constitute real-time monitoring of a range of environments that are both lawful and constructive. To close this IGA, we urge an assessment of the use of technologies, with an emphasis on their place as tools built into a robust SIF that is mission-agnostic but readily adapted to a diverse set of IC and LE needs.

2.2 Organizational

IGA seams also exist in organizations themselves. Ideally, the IC should be an adaptive, diverse, and nimble composite capable of working as the senses of the Nation's security and defense interests. In practice, however, the IC is resistant to change, either out of disagreement with the need or perceiving itself as immune from criticism (Wardlaw, 2015).

For purposes of understanding organization agent roles, we use a typological range of agent types was defined as "alpha," "beta," and "gamma" actors (Alessa & Kliskey, 2012). Alpha actors tend to act as initiators of change response, betas as supporters, and gammas exhibit opportunistic reactions, or serve as detractors. This range bears similarities to Equiluz' personality types of "satisfied cooperators (leaders)," "unsatisfied cooperators (conformists)," and "defectors taking advantage (exploiters) (Zimmerman & Equiluz, 2005)," though with increased specificity and increased emphasis on the agents' role within a group (e.g., formal and informal leadership, facilitative, and obstructive functions), and the agent's focus on individual or collective gain.

Agents of change (generally alpha agents) are often at a significant disadvantage and experience poor receptivity and, in some cases, outright hostility (Campbell et al., 2015). Several studies and reports have pointed to this phenomenon as one deeply rooted in the factors, such as leadership failure, where a workforce is willing, or instances where leadership goals are at odds with a workforce that perceives change to equate to job-insecurity and/or a measure of their self-worth as opposed to an opportunity to learn new skills, transfer a wealth of tacit and implicit knowledge, and engage adversaries on equal footing (Pardo Del Val & Fuentes, 2003). Research at community and organizational scales suggest that it is only active or inadvertently impeding actors, the *gamma actors*, who can disproportionately and negatively affect the pace of innovation (Alessa & Kliskey, 2012). The gamma actor often

accomplishes this in order to maintain the *status quo* to which they have become accustomed, to avoid a personal sense of failure, inadequacy or fear, and/or a sense of power/ego (Peters, 2009). When gamma actors occupy supervisory or leadership positions, they impede the progress of both people and the mission they serve creating vulnerabilities through inaction or inappropriate words and/or actions that, in aggregate, are damaging to the Nation (Maras, 2017; Studeman, 2007). Dissent and argumentation are essential components of the U.S. macrostructure, but gamma actors intentionally cross-link intense structural, personal, and organizational conflict that is difficult to disambiguate, breaking down and confusing communication and coordination across efforts. This perpetuates a culture that does not support diverse perspectives, multimodal approaches, or different ways of thinking.

To more fully understand the Organizational IGA, we used the QED to create trust spaces in which the practitioners could easily adapt to working across multiple cultures (or tribes) where each culture is retained and yet, a mission-centric assessment could be attained. The QED is the starting point of the SIF shown in Figure 2 because it establishes the plurality of rulesets, reflecting the tacit and implicit knowledge across the FSLTTPP IC and LE

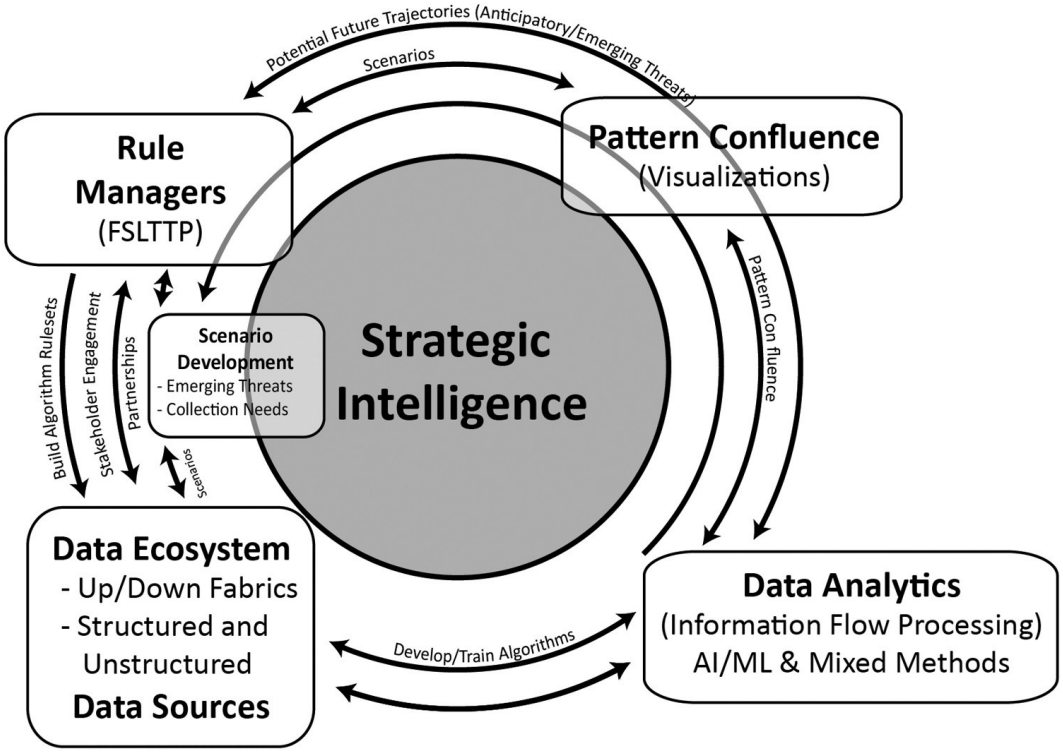

Figure 2. The strategic intelligence framework used by the big data analytics for decision support team. The visualization front-end, Mesoscale operational situational awareness intelligence composite, was co-designed with operators and policy makers across the US intelligence community and law enforcement communities and is being applied in the field by operational components of the US Department of Homeland Security.

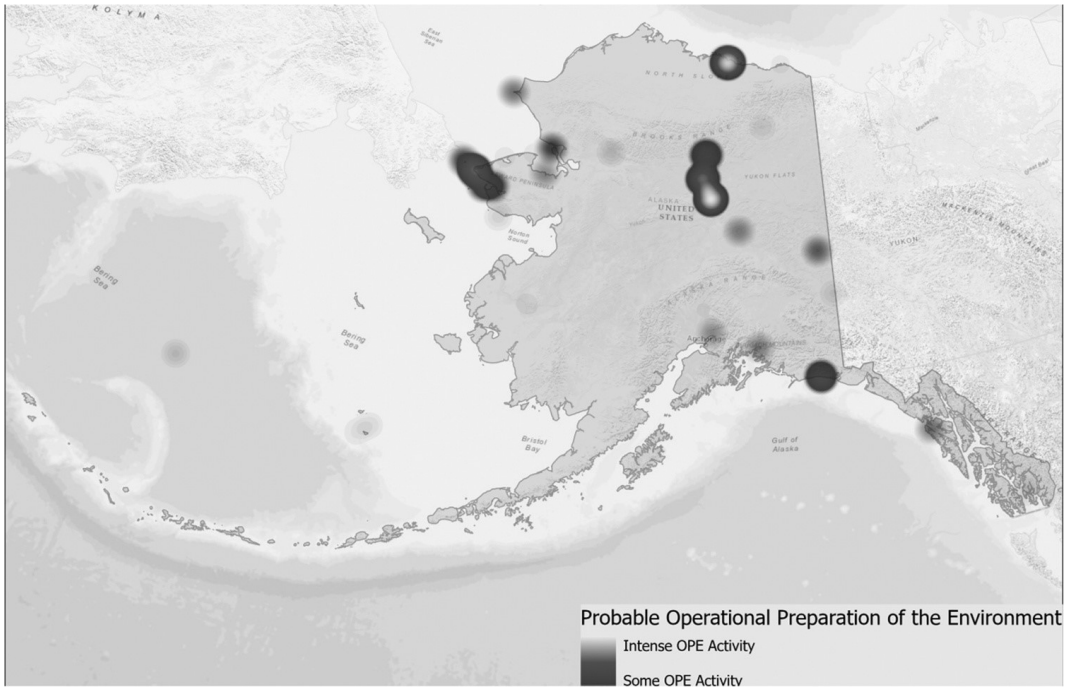

Figure 3. Example Mesoscale operational situational awareness intelligence composite developed using open-source intelligence to evaluate levels of activity potentially indicated asymmetric competition activities in the U.S. Arctic and Alaska.

communities (Alessa et al., 2018a). It is through such means, whereby small changes accrue, that we are rapidly able to acquire awareness of adversarial IGA activities and mount denial and defense. For example, we identified a series of specific vulnerabilities available for adversary exploitation that included:

(a) **The ability to gain access** to our academic enterprise writ large, which allows passive and active nefarious information flows to shift and shape attitudes toward collaboration and creative potential for future development and transition to gain economic, strategic and/or military benefit ahead of the United States (Coats, 2018).
(b) **Operating as a collective data and information gathering network** to acquire pattern of life (POL) throughout the FVEYs partners (United States, the United Kingdom, Canada, Australia, and New Zealand), nefarious actor networks are capable of continuously streaming acquired information for rapid synthesis and analysis by adversaries, including Nation States, to advance larger, more global goals against which no technology can defend (Coats, 2018).

(c) **The ability to outcompete** us in the transition of stolen intellectual property from research and development to deployment, production and/or shipping on a global scale means that a competitive advantage is perpetually maintained.
(d) **Investments in critical infrastructure and capabilities** that appear to be narrowly focused but instead are multi-purposed to provide a licit and legal cover for activities designed to harm and/or otherwise be illicit in aggregate.
(e) **Adversaries' ability to use laws and policies** against us in support of their own agenda. Laws and policies in democracies versus authoritarian nations allow a more permissive environment for asymmetric competition activities to occur.

The seam within the organizational IGA is further exacerbated by potentially well-intentioned Government agencies that promote the scientific sharing of data in areas that are ultimately sensitive and could pose grave risk to the Nation in aggregate (see https://vimeo.com/473452893). By way of example, consider Arctic science, especially that focused on oceanography (e.g., bathymetry), sea ice, food (especially fisheries), energy, water, language, geomorphology, subglacial lakes, and permafrost (Department of State, 2017). Scientific Cooperation Agreements and other cooperative memorandums can advance global understanding of the Arctic environment but run the risk of disproportionately revealing information that may harm national security (Berkman & Vyelgzhanin, 2012). Several authors have called out the problem but have focused narrowly on military interactions (Forsyth, 2018; Maras, 2017) and the USG has responded by engaging in awareness campaigns, increased scrutiny of visas, attempting to tighten export controls, and attempting to regulate scientific activities. Each of these has had limited success (Kraska & Baker, 2014) in part due to the majority of IGA activities occurring outside these authorities and in part because they have alerted adversaries to the tactics resulting in adaptation. The USG has currently failed to address IGAs and has no comprehensive strategic plan or policies for doing so (Holland, Cunningham, & Vagg, 2013). It was only in the waning hours of the 45th Presidency that the USG was directed to do so with respect to government supported research and development, a single sector of the overall problem (NSTC, 2021; Office of the White House, 2021). This has left it to individual universities, research agencies, and companies to navigate this emerging and complex risk landscape, often with increased awareness but facing a difficult balance upholding international freedoms, fairness, and democratic values while interpreting and executing the messages delivered by the USG. Compounding this is the real and present danger of penalizing legitimate collaborations by subjecting them to prejudice through perception of association.

2.3 Information (Data and analytics)

The Information (Data and Analytics) IGA (Information IGA) extends across and perpetuates the Operational and Organizational IGAs. It is the result of the low data diversity, particularly at local scales, as a result of rapidly built-out observational systems (e.g., the industry tail wagging the defense/national security dog), overly restrictive, low-fidelity policies around information and data sharing (Kshetri, 2014), and the cultures inherent in various data tribes. Directly impacting the Informational IGA is a classic case of the old programmers' adage: garbage in/garbage out. Many IC practitioners still believe that a model equates to analytics. To better understand this, as noted earlier, 12 QED workshops were conducted over three years, from 2016 to 2019 (See "1.2 QED Workshops – Selected Overviews). They brought together diverse stakeholders to determine data, framework, and analysis requirements (Alessa et al., 2017a; 2017b, 2017c, 2017d, 2018b, 2018c, 2018d, Alessa & Moon 2020). Additional QED workshops were held in the same time frame, focused on generating statistically significant results related to risk environments, technology impacts, and other related topics. Of specific note to the Information IGA were the November 2017 *Central America Pacific Rim Risk Intersections*, March 2018 *Data Integration and Information Sharing*, and April 2018 *Improved Data Access/Fusion/Sharing for Joint Task Forces* workshops. In these session, groups of subject matter experts convened in Washington DC and sought clarity on the types of data streams available to decision makers, analysts and operators involved in addressing IGAs, as well as impediments to their utility. The results reflect three general conclusions:

(a) **Our focus on media mining**, particularly attempting to quantify sentiments using social media to then quantify values, perceptions, and behavior, is potentially dangerous and has little return on investment: disinformation and designed decoys constitute a significant amount of the information the IC uses in its analyses (Alessa & Valentine, 2020; Bennett & Livingston, 2018). A more integrative approach should consider a range of metrics, including physical proxies for social dynamics, and based in resilience science (Williams et al., 2018).
(b) **Our focus on seeking artificial intelligence "solutions"** is misguided - we must do a better job training the IC to ask better questions. The quest for the "magic button" has only resulted in a degradation of the intelligence tradecraft and a failure to recognize that a science of security is necessary to enable analytic technologies (Alessa et al., Forthcoming).

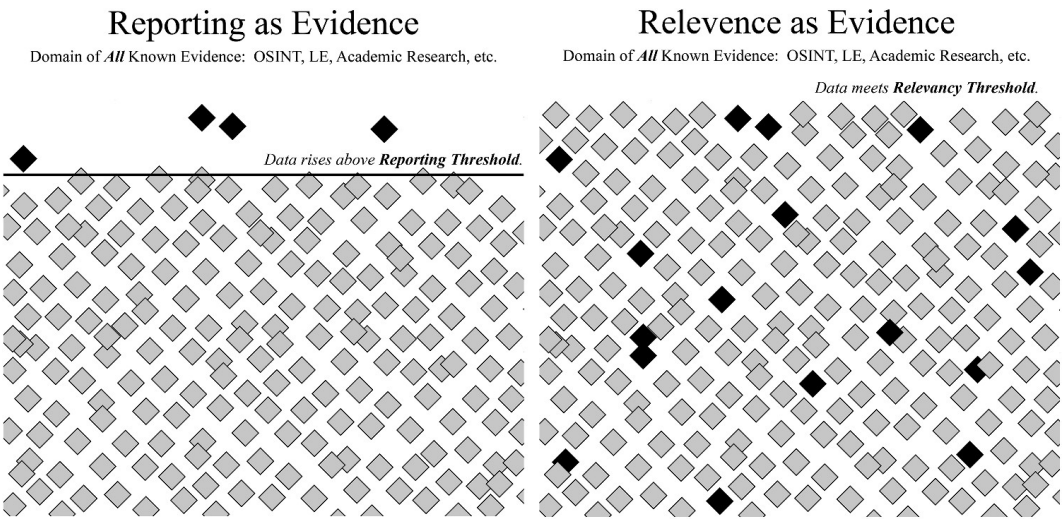

Figure 4. Diagram highlighting the difference between reporting of observations as data compared to relevance of observations as data.

(c) **We do not use a systems science approach for the intelligence enterprise**. It is still built on the principles of political science and international relations that Kent developed during World War II (Davis, 2002). Instead, we rely on study groups, think tanks, media reports, and published books.

As a result of these legacies and missteps, we have over-invested in observing, surveillance and monitoring systems at larger regional scales that do not provide enough context or resolution at smaller, local scales necessary to identify, predict, and respond to the types of adversarial or IW/OPE activities occurring in IGAs. In other words, we lack the ability to resolve activities at local scales that may be part of IW/OPE which is exactly the scales at which such activities would occur (Kilcullen, 2019; Ucko & Marks, 2018). Capabilities that have been built to address this successfully have promptly been squashed by agencies such as the U.S. Coast Guard whose agenda toward investment in equipment is inconsistent with established and proven innovation such as community based/community enabled observing networks (Alessa et al., 2015; Griffith et al., 2017). Ultimately, the data and information IGA has emerged because we have not, historically, examined the signals hidden in the noise, essentially the spaces *between* data shapes and nodes (Wasserman, 2018). This, in turn, has shaped a misconception that *reporting* is synonymous with *evidence*. While reporting is a type of evidence, IGAs present signals hidden in noise, often undetectable by our current reporting methodologies (Figure 4).

3. How do we avoid surprise?

If we are to avoid further catastrophic surprise in the future the U.S. intelligence, defense, and security enterprise will need to have the resolve and courage to make simple changes that will allow it to reveal these signals hidden in the noise, make sense of them, and act more quickly to avoid surprises in the future. We offer six pivotal elements that can be rapidly addressed to enhance and enable adaptation across the U.S. intelligence enterprise; however, we caution that examining these elements will require difficult conversations, strong leadership both from above and across organizations, a spirit of cooperation and service, and a reexamination of fundamental assumptions about the value and effectiveness of our current intelligence frameworks and information models:

(a) **Reexamine archaic authorities**: IGA warfare in its most sophisticated form means the adversary has acquired deep knowledge of our POL, and they understand laws and policies better than the majority of citizens, including law enforcement agencies (LEA). The adversary then exploits these POL to achieve their goals. In our current construct of authorities, the hidden nature of these actions makes identification and response fundamentally a counterintelligence (CI) mission which falls primarily to the Federal Bureau of Investigation (FBI) within the DOJ, the Central Intelligence Agency (CIA), as well as the DOD's Defense Counterintelligence Security Agency. While the FBI has an extensive and decorated history of CI skillsets that can be resourced, building them out with more innovation and diversity has not yet occurred. This is a needed first step to address in IGAs on domestic soil. Similarly, the CIA and the DOD also have very mature CI capabilities that can be focused on IGAs and can train organizations with domestic responsibilities on how to identify and combat IGA actions. Other LEAs, such as the LE components of the DHS, specifically Border Patrol and Homeland Security Investigations, offer additional and diverse skillsets which, through honestly brokered partnerships, could ensure greater continuity of information and interdiction. To this point, several Border Patrol Sectors have already adapted to regionally changing threat landscapes through their Sector Intelligence Units (SIUs), which work through engagement with local communities and partners to develop systematic and transparent protocols. They have done this adaptively and sometimes despite rigid, centralized entities within DHS. Such a model could create a more cohesive and dedicated domestic CI workforce that is charged with protecting freedom and privacy while denying adversary activities that work to dismantle systems within which such freedoms and privacy can exist.

(b) **Call out conflicts of will and perceptions of change**: Agencies often promote narratives that point to their desire to adapt but, due to a range of constraints discussed below, fail to execute the majority of actions that can enable an agile workforce. In part, as noted previously, this is an internal struggle either between leadership failures, where a workforce is willing, or leadership goals and a workforce that perceives change to equate to job-insecurity and/or a measure of their self-worth (Pardo Del Val & Fuentes, 2003). Only by engaging in difficult dialogs about what adaptation means at the individual versus organizational scale will it be possible to fully realize that the cornerstone of organizations – their people – can gain the knowledge to embrace complexity and think critically about key problems and apply a security science in order to find lawful and adaptive solutions that provide a comprehensive, government-wide plan for defense in the IGAs.

(c) **Clarify artificial dichotomies between Nation State activities and activities out of context**: Threats emerge at different rates from different sources. The United States, by choice, creates a duality of state and non-state actors as well as inherently divided authorities and jurisdictions. This creates a bifurcation between irregular activities, often in compliance with our laws, and conventional operations we readily recognize as conflict or crime (Ucko & Marks, 2018). The gap between these two creates a self-inflicted IGA precisely because of the lag in addressing the fundamental issues above: we cannot see the activity, if we could we would not recognize it; we lack an apparatus to respond, and even if we had the apparatus, the authorities to address these actions are lacking or unclear. We suggest a formal joint strategy be developed by DHS and the DOJ, with support from the DOD and IC for identifying, preventing, disrupting, and responding to domestic IW/OPE activities. This strategy should include a quantitative (versus descriptive) assessment of current presumptive competitor activities and possible ways to address them, including legislative changes that could be made without sacrificing the diplomacy and global commons of economic partnerships in a globalized world.

(d) **Re-vamp an IC workforce to ensure qualifications match missions**: Taken as a whole, the USG possesses relatively limited science, technology, engineering and/or mathematics expertise, relying instead on partnerships with academia and the private sector (Chang & Tetlock, 2016). Such scientific illiteracy is a consequence of Kent's construct and a legacy of past wars. It is compounded by a lack of access to the appropriate training, defaulting to legacy programs which do little to diversify skillsets. As a result, many IC members regularly confound information with 'data' and spreadsheet manipulations with 'data

science' because they are not scientifically trained. This scientific literacy insufficiency compounds the challenges to the IC's ability and likelihood of success, and of accurately determining its research, development, and technology needs in the immediate, near-, and long-term. Real-world data are noisy, messy and drift over time (Stobierski, 2021), requiring extensive cleaning and wrangling also known as remediation. Modern data science methods can easily handle this, but the IC works off a limited set of integrated, end-to-end data frameworks, most of which would not pass academic review, and in fact has as a stated objective establishing a common reference data architecture (Office of the Director of National Intelligence (ODNI), 2017). Our failure to invest in rigorous, integrative social science means we build scenarios that cannot be modeled. This renders the nation blind because actions because a data-driven, systems science backed means to derive value from data as an ecosystem and identify emerging threats as an on-going enterprise is simply not currently in place. Compounding this is the fact that information is often over classified and rendered inaccessible to those operators and law enforcement officers who could detect such activities more effectively. Recently, pushed out of their sensitive compartmented information facilities (SCIFs) a portion of the IC has been forced to quickly learn open-source intelligence (OSINT) techniques. Circling back to the lack of scientific training and having looked down on OSINT in the past, the IC may be introducing a new range of vulnerabilities into the U.S. intelligence enterprise. We urge the IC to make better use of a variety of means to diversify the expertise and knowledge base across the IC and LE communities, taking advantage of statutes and laws, such as the Intergovernmental Personnel Act (Public Law 91–648), to establish an Intelligence Community Academic network (ICAN) as well as training a broad cadre of state and local law enforcement officers in IW/OPE doctrine, systems, and complexity science, and indicators so as to more rapidly detect them.

(e) **Reexamine the cultural bias toward purchasing high cost "solutions looking for a problem"** vice defining analytic problems and then seeking solutions. The former mind-set has created the perception that hardware and software constitute an end rather than a means. Further, uncoordinated expenditures on often low-return RD investments take valuable resources away from programs, which are necessary for a diversity of information, data, and experience. Relying on such purported, and often misleadingly marketed, products tends to allow commercial sectors to drive government planning and place many agencies' intelligence and law enforcement efforts at a disadvantage when evaluating the science behind the systems and frameworks they use (Committee on the Future U.S. Workforce for Geospatial

Intelligence (CFUSWGI), 2013; Gates et al., 2008). As a result, trillions of dollars are spent on technologies despite the lack of a rigorous and cohesive scientific framework that adds value or enhances cohesion across the USG interagency. For example, the technology surrounding government scanning of in-bound cargo and vehicles at borders and ports are driven by an industry-defined state of the art instead of the government-defined state of desirability (Government Accountability Office (GAO), 2013). While government use of re-purposed industry solutions is understandable given the expenses of research and development, this tail-wagging-the-dog scenario has opened several vulnerabilities (Voelz, 2006): if the enterprise is highly reliant on purchased operational technologies (OT), and the industry is known to be compromised (Davies, 2005; Marrin, 2001) we must logically entertain the hypothesis that our adversaries may have herded us into a "buffalo jump" of technologies, which equalize rapidly, for their own benefit. A Buffalo Jump is a term tied to the gradual modification of both academic/industry knowledge engines such that security and defense agencies adopt technologies without an overall strategic framework. Buffalo jumps are a core component of irregular warfare that we hypothesize have been used against us but are beyond the scope of this paper.

(f) **Implement A Framework for Getting Ahead of Asymmetric Surprise**. As the IGA landscapes grow increasingly more complex, we are increasingly at risk of being faced with eruptive events for which we are unprepared. Investing more fully in computational social science (e.g., the COMSES Network, https://www.comses.net) will allow us to more accurately model a range of scenarios that may produce surprises. This will be a significant step forward to enable us to identify how, when, where, and why adversarial actions are occurring. In other words, intelligence is a fundamentally human enterprise that should be augmented using machines through a range of analytic tools with outputs of pattern confluence (e.g., MOSAIC). The outputs have greater utility: they can be readily digested, used, shared, and updated in real-time, reducing the need to create standardized data architectures (thus losing potentially useful data) or creating a common data ingest. To put it another way, whether the concern is weapons of mass destruction or attacks on supply chains, such a framework helps address the question "how do we avoid surprise?" by ensuring that activities which occur in IGAs are fully illuminated for early warnings against attack.

Overall, our inability to detect signals hidden in perceived irrelevant data or "noise" has inadvertently allowed IGAs to become wider than we are able to detect. This ranges from our ability to reveal IW/OPE patterns (i.e., precise, or "exquisite" awareness) to the ability to operationally deny the adversary access to our most critical assets, natural resources such as farmland and freshwater, as well as infrastructures, freedoms, and ideas on our own soil. In other words, our homeland is no longer a sanctuary until we make it so again by learning from the past, adapting in the present and using sound scientific strategic frameworks to forecast the future (Alessa et al., Forthcoming).

4. Back to the future

The need for establishing a security science discipline has been outlined recently (Alessa et al., Forthcoming). Briefly, this would build off the processes and scientific method of hypothesis testing in the construct of complex adaptive systems. It would not replace existing intelligence methods but rather introduce a level of rigor compatible with the tools and technologies of advanced analytics such as artificial intelligence and machine learning. Such an evolution is critical: Without mastery of foundational quantitative science principles, no technological tool can be utilized to its potential. However, illuminating adversarial activities in the IGAs earlier will also require culture changes in the law enforcement, intelligence, defense, and homeland security enterprises. We will need to "get over ourselves," and cooperate to connect the dots in new ways. For example, combining the CI authorities and expertise of the FBI with the IW/OPE expertise of the academic and special operations community, and the place-specific, contextual knowledge of local LEA and communities. Some have advised that such a configuration is a "unicorn," something that cannot exist in reality. We assert that this is merely a failure to think adaptively, engage in a revision of policies, and meet the new threat landscape with a clear vision and a unity of effort that restores the United States to its position of strength through diplomacy and partnerships while simultaneously protecting our homeland.

Note

1. Much like "great power competition", "irregular warfare" and "operational preparation of the environment" (IW/OPE, sometimes also referred to as "IW/UW/PW") lacks a consensus definition or suite of meanings. Regardless, "IW/OPE" refers to activities that are often licit and legal for the purpose of acquiring information, resources and/or influence so as to give an adversary the advantage. This manuscript takes into account the multitude of roles the IC has, from law enforcement to support of defense activities. Ensuring these roles are realized requires quantitative systems science to tangibly define,

demonstrate and test the variables and their dynamics in IW/OPE. To accomplish this a qualified workforce and appropriate technologies must be acquired.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was partially supported by the US National Science Foundation [1927713]; US National Science Foundation [1642847].

Notes on contributors

Dr Lilian "Doc" Alessa is a President's Professor at the University of Idaho and has served as a Defense Intelligence Senior Level (DISL) Advisor for Advanced Data and Analysis, through an Intergovernmental Personnel Act (IPA), with the Department of Defense. Additionally, she served as Deputy Chief of Global Strategies with the Department of Homeland Security, Office of Strategy, Policy and Plans. She has over 25 years of experience working with diverse partners across Canada and the United States, providing data-intensive decision support tools to improve the resilience of systems, people and communities focusing on the biophysical, social, psychological and strategic aspects of security and defense. She has led several multi-million dollar data integration/data fusion programs working closely with Federal agencies. An internationally recognized expert in resilience, early warning systems and remote regions, she sits on several national committees and has led the development of two joint Canada-United States Arctic resilience toolbox assessments. She is one of the Co-Founders for the Community of Modeling in Social Ecological Systems (COMSES), hosted out of Arizona State University (comses.net). Dr. Alessa has been working across the U.S. interagency providing subject matter expertise on issues related to Covid19 and domestic resilience in the context of the Peoples' Republic of China.

Mr Sean Moon is the Chief of Global Strategies in the U. S. Department of Homeland Security Office of Strategy, Policy, and Plans, Washington, D.C. Among other projects in his portfolio, he is the Policy lead for Arctic strategy development. Between 2011 and 2016, he served the Department 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 U.S. 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.

CMDR James 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 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).

Mr Michael Marks holds a Juris Doctorate from the University of Florida College of Law and has authored books and interactive programs that have been integrated into emergency response certification requirements in 27 states, to include notable adoption within: U.S. Army Special Operations Command, the FBI, the DEA, the CIA, HIDTA and the U.S. Secret Service. He independently authored The Emergency Responder's Guide to Terrorism which was adopted by such entities as the State of New York, the International Fire Service Training Association, Oklahoma State University, George Washington University, the American College of Forensic Examiners, the Federal Law Enforcement Training Center and the U.S. Army / FBI Hazardous Devices School. He served for twelve years as an Adjunct Professor at the George Washington University College of Forensic Science focused on Continuity and Response to Weapons of Mass Destruction. In 2008 he authored a Master's Degree in Homeland Security curricula for Universitá Guglielmo Marconi, Rome, Italy.

Mr Don Hepburn is a highly decorated intelligence veteran and US national security expert. Serving nearly thirty years with the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) he retired at the rank of Senior Intelligence Service Officer. During government service Mr. Hepburn held executive positions in both the field and Washington D. C. His foreign field deployments included command positions as Chief of Station and Chief of Base. In CIA Headquarters he served as Task Force Chief and Chief of a Middle East Group directing CIA's leadership teams and intelligence operations over multiple countries. In the FBI he served as the Deputy Assistant Director of the International Operations Division. Mr. Hepburn obtained his BA from the University of Southern California, Los Angeles and his MA from Columbia University, New York. He is the recipient of the CIA Director's Award, the Distinguished Career Intelligence Medal and the CIA Meritorious Unit Citation for Intelligence.

Dr Andy Kliskey is President's Professor and Co-Director of the University of Idaho Center for Resilient Communities (CRC). Kliskey is also the Idaho EPSCoR Project 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 last 20 years working in indigenous and rural communities in Alaska, British Columbia, Hawaii, Idaho, New Zealand, and the Yukon examining community and landscape resilience. His teaching and research is interdisciplinary in nature and directed at integrated methodologies in social-ecological systems that combines stakeholder-engagement, scenario analysis, and geospatial modeling. Kliskey is a project lead on two NSF Innovations at the Nexus of Food, Energy, and Water Systems (INFEWS) awards.

References

The 9/11 Commission. (2004). *The 9/11 Commission Report*, Government Printing Office, Washington, DC. https://govinfo.library.unt.edu/911/report/911Report_Ch11.pdf .

Adomavicius, G., & Tuzhilin, A. (2005). Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. *IEEE Transactions on Knowledge and Data Engineering*, *17*(6), 734–749. doi:10.1109/TKDE.2005.99

Aid, M. (2011, August). Sins of omission and commission: Strategic cultural factors and US intelligence failures during the cold war. *Intelligence and National Security*, *26*(4), 478–494. doi:10.1080/02684527.2011.580602

Alessa, L., & Kliskey, A. (2012). The role of agent types in detecting and responding to environmental change. *Human Organization*, *71*(1), 1–10. doi:10.17730/humo.71.1.y7692065g232w1g1

Alessa, L., Kliskey, A., Gamble, J., Fidel, M., Beaujean, G., & Gosz, J. (2015). The role of indigenous science and local knowledge in integrated observing systems: Moving toward adaptive capacity indices and early warning systems. *Sustainability Science*, *11*(1), 91–102. doi:10.1007/s11625-015-0295-7

Alessa, L., & Moon, S. (2018c). *Rapid Results Report of the DHS Improved Data Access/Fusion/Sharing for JTFs Workshop*. Center for Resilient Communities, University of Idaho, Moscow, ID, United States of America.

Alessa, L., & Moon, S. (2020). *Arctic Trix (ArcTrix) Workshop Report*. Center for Resilient Communities, University of Idaho, Moscow, ID, United States of America.

Alessa, L., Moon, S., & Bielby, M. (2017d). *Report of the Central America Pacific Rim Risk Intersections (CAPRRI) Workshop*. Center for Resilient Communities, University of Idaho, Moscow, ID, United States of America.

Alessa, L., Moon, S., Griffith, D., & Kliskey, A. (2017c). *Report of the Port of San Diego Vulnerability Assessment and Security Workshop*. Center for Resilient Communities, University of Idaho, Moscow, ID, United States of America.

Alessa, L., Moon, S., Griffith, D., & Kliskey, A. (2018a). Operator driven policy: Deriving action from data using the quadrant enabled Delphi (QED) method. *Homeland Security Affairs Journal*, *14*(6). https://www.hsaj.org/articles/14586

Alessa, L., Moon, S., Griffith, D., & Kliskey, A. (2018d). *Report on the coastal observing data and information sharing for security workshop*. Center for Resilient Communities, University of Idaho, Moscow, ID, United States of America.

Alessa, L., Moon, S., Griffith, D., Kliskey, A., & Bielby, M. (2017a). *Report of the Emerging Arctic Security Threats Matrix (EarthX) for Improved Canada-United States (CANUS) Arctic Security Workshop*. Center for Resilient Communities, University of Idaho, Moscow, ID, United States of America.

Alessa, L., Moon, S., Griffith, D., Kliskey, A., & Bielby, M. (2017b). *Report of the Northern Border Security Review Workshop*. Center for Resilient Communities, University of Idaho, Moscow, ID, United States of America.

Alessa, L., Moon, S., Griffith, D., Kliskey, A., & Bielby, M. (2018b). *Report of the Data Interoperability Information Sharing (DIIS) Workshop*. Center for Resilient Communities, University of Idaho.

Alessa, L., Moon, S. K., Valentine, J., and Kliskey, A. (Forthcoming). Detecting asymmetric competition by China in the United States and Canadian Arctic. *Journal of Indo-Pacific Affairs*.

Alessa, L., & Valentine, J. (2020). Truth and trust must prevail over disinformation about the pandemic. The Hill, April 26, 2020. https://thehill.com/opinion/national-security/493985-truth-and-trust-must-prevail-over-disinformation-about-the-pandemic

Alessa, L., Williams, P., Kliskey, A., & Beaujean, G. (2016). Incorporating community-based observing networks and systems: Toward a regional early warning system for enhanced responses to arctic critical events. *Washington Journal of Environmental Law and Policy*, *6*(1), 1–27.

Barrett, D., & Zapotosky, M. (2021). FBI report warned of 'war' at Capitol, contradicting claims there was no indication of looming violence. *The Washington Post*, January 12, 2021. https://www.washingtonpost.com/national-security/capitol-riot-fbi-intelligence/2021/01/12/30d12748-546b-11eb-a817-e5e7f8a406d6_story.html .

Bennett, W., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, *33*(2), 122–139. doi:10.1177/0267323118760317

Berkman, P., & Vylegzhanin. (Eds.). (2012). *Environmental security in the Arctic Ocean*. Routledge; London, United Kingdom.

Bracken, P. (2006). *Net assessment: A practical guide*. The Commonwealth Institute of Cambridge, MA, USA, Archived by the Project of Defense Alternatives. Retrieved January 13, 2021. https://www.comw.org/qdr/fulltext/06bracken.pdf .

Campbell, K. S., Carmichael, P., & Naidoo, J. S. (2015). Responding to hostility: Evidence based guidance for communication during planned organizational change. *Business and Professional Communication Quarterly*, *78*(2), 197–214. doi:10.1177/2329490614551570

Chang, W., & Tetlock, P. E. (2016). Rethinking the training of intelligence analysts. *Intelligence and National Security*, *31*(6), 903–920. doi:10.1080/02684527.2016.1147164

Chappell, B., Myre, G., & Wamsley, L. (2020). What We Know About Russia's Alleged Hack of the U.S. Government and Tech Companies, National Public Radio, December 21, 2020. Retrieved January 14, 2021. https://www.npr.org/2020/12/15/946776718/u-s-scrambles-to-understand-major-computer-hack-but-says-little .

Clark, B., Patt, D., & Walton, T. (2020). The department of defense needs to relearn the (Almost) lost art of net assessment. The Strategy Bridge, November 19, 2020. https://thestrategybridge.org/the-bridge/2020/11/19/the-department-of-defense-needs-to-relearn-the-almost-lost-art-of-net-assessment .

Coats, D. (2018). *Director of National Intelligence's Statement for the Record: Worldwide Threat Assessment of the U.S. Intelligence Community*, January 29, 2018 (Testimony Date).

Committee on the Future U.S. Workforce for Geospatial Intelligence (CFUSWGI). (2013). *Future U.S. Workforce for Geospatial Intelligence*. The National Academies Press; Washington, DC, United States.

Custer, R. L., Scarcella, J. A., & Stewart, B. R. (1999). The modified Delphi technique - A rotational modification. *Journal of Vocational and Technical Education*, *15*(2), Retrieved March 5, 2010 Spring 1999. http://scholar.lib.vt.edu/ejournals/JVTE/v15n2/custer.html/

Davies, P. (2005). Intelligence, information technology, and information warfare. *Annual Review of Information Science and Technology*, *36*(1), 312–352. doi:10.1002/aris.1440360108

Davis, J. (2002). Sherman Kent and the Profession of Intelligence Analysis, Central Intelligence Agency. *Kent Center Occasional Papers*, 1 (5), November 2002. https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm

Department of Homeland Security (DHS). (2014). *U.S. Department of Homeland Security Quadrennial Homeland Security Review*. https://www.dhs.gov/publication/2014-quadrennial-homeland-security-review-qhsr

Department of Justice (DOJ). (2018). *The United States Department of Justice Mission Statement*, January 30, 2018 https://www.justice.gov/about .

Department of State. (2017). *Agreement on Enhancing International Arctic Scientific Cooperation*. Author. https://www.state.gov/e/oes/rls/other/2017/270809.htm .

Dilinian, K. (2012). U.S. Intelligence Official Acknowledges Missed Arab Spring Signs, *Los Angeles Times*, July 19, 2012, https://latimesblogs.latimes.com/world_now/2012/07/us-intelligence-official-acknowledges-missed-signs-ahead-of-Arab-spring-.html .

Dobbins, J., Scobell, A., Burke, E., Gompert, D., Grossman, D., Heginbotham, E., & Shatz, H. (2017). *Conflict with China revisited: Prospects, consequences, and strategies for deterrence*. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/perspectives/PE248.html

Dunn-Cavelty, M., & Mauer, V. (2009, April 1). Postmodern intelligence: Strategic warning in an age of reflexive intelligence. *Security Dialogue*, *40*(2), 123–144. doi:10.1177/0967010609103071

Dupont, A. (2020). The US-China cold war has already started. *The Diplomat*. July 8, 2020. https://thediplomat.com/2020/07/the-us-China-cold-war-has-already-started/

Erwin, M., & Belasco, A. (2013). *Intelligence spending and appropriations: Issues for congress*. Congressional Research Service; Washington, DC, United States of America. 7-5700, R42061 https://fas.org/sgp/crs/intel/R44381.pdf

Everett, B., & Gerstein, J. (2014). Why Didn't the U.S. Know Sooner?, Politico, March 5, 2014, https://www.politico.com/story/2014/03/united-states-barack-obama-Ukraine-crimea-Russia-vladimir-putin-104264 .

Federation of American Scientists. (2021). *The Evolution of the U.S. Intelligence Community-An Historical Overview*, Retrieved January 11, 2021. https://fas.org/irp/offdocs/int022.html

Forsyth, M. (2018). Why Alaska and the Arctic are critical to the national security of the United States. *Military Review*, 114: 113-119. January-February 2018.

Fruhlinger, J. (2020). The OPM Hack Explained: Bad Security Practices Meet China's Captain America | CSO Online, Chief Security Officer (CSO) by International Data Group (IDG), February 12, 2020, https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html .

Galinec, D., & Macanga, D. (2012). Observe, orient, decide and act cycle and pattern-based strategy: Characteristics and complementation. *Central European Conference on Information and Intelligent Systems*, 371–378. Varazdin, Croatia.

Garten, J. W. (2019). The future of analysis. *Studies in Intelligence*, *63*(2). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol-63-no-2/Future-of-Analysis.html

Gates, S., E. Keating, A., Jewell, L., Daugherty, B., Tysinger, A., Robbert, R., & Masi, R. (2008). *The Defense Acquisition Workforce: An Analysis of Personnel Trends Relevant to Policy, 1993–2006*. RAND Corporation TR-572-OSD.

Gentry, J. A., & Gordon, J. S. (2019). *Strategic warning intelligence: History, challenges, and prospect*. Georgetown University Press; Washington, DC, United States of America.

Gertz, B. (2016). Office of No Threat Assessment, The Washington Times, August 24, 2016. https://www.washingtontimes.com/news/2016/aug/24/pentagons-offic-of-threat-assement-under-fire-from/

Glasser, S. (2017). Ex-Spy Chief: Russia's Election Hacking Was An 'Intelligence Failure,' POLITICO Magazine, December 11, 2017, http://politi.co/2AJK9gW .

Government Accountability Office (GAO). (2013). *Combating Nuclear Smuggling: Lessons Learned from Cancelled Radiation Portal Monitor Program Could Help Future Acquisitions* (Report No. GAO-13-256), Government Accountability Office.

Grewe, B. A. (2004). *Legal Barriers to Information Sharing: The Erection of a Wall Between Intelligence and Law Enforcement Investigations, Commission on Terrorist Attacks Upon the United States*, Staff Monograph, August 20, 2004, declassified May 20, 2009. https://fas.org/irp/eprint/wall.pdf

Griffith, D., Alessa, L., & Kliskey, A. (2017). A typology of community-based observing. *NIMIO Bulletin*, *12*(1), 32–39.

Hedley, J. (2005). Learning from intelligence failures. *International Journal of Intelligence and CounterIntelligence*, *18*(3), 435–450. (October 2005). doi:10.1080/08850600590945416

Helal, H., & Hassan, O. (2017). Maritime surveillance: An integral part of maritime security. In A. Khondaker (Ed.), *Land and maritime border security and safety: Challenges and solutions* (pp. 184–194). Saudi Border Guard; Jeddah, Saudi Arabia.

Hepburn, D. (2018). *Foreign agents infiltrated life in America, unseen and unchecked*. The Hill, December 18, 2018. https://itk.thehill.com/opinion/national-security/421500-foreign-agents-infiltrated-life-in-america-unseen-and-unchecked

Holland, A., Cunningham, N., & Vagg, X. (2013). *Critical security challenges in the Arctic*. American Security Project. https://www.eenews.net/assets/2013/09/19/document_cw_02.pdf

Hoover Institution. (2004). *Policy Review*: Intelligence Failures, February 1, 2004. https://www.hoover.org/research/intelligence-failures .

Kardos, M., & Dexter, P. (2017). A Simple Handbook for Non-Traditional Red Teaming, Joint and Operations Analysis Division, Commonwealth of Australia Department of Defence, Science and Technology, DST-Group-TR-3335, January, 2017. https://apps.dtic.mil/dtic/tr/fulltext/u2/1027344.pdf

Kilcullen, D. (2019). The evolution of unconventional warfare. *Scandinavian Journal of Military Studies*, *2*(1), 61–71. doi:10.31374/sjms.35

Kindsvater, L. C. (2008). The need to reorganize the intelligence community, a senior officer's perspective. *Studies in Intelligence*, *47*(1). https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article03.html

Kiras, J. (2016). Irregular warfare: Terrorism and insurgency. In D. Jordan, J. Kiras, D. Lonsdale, I. Speller, C. Tucker, & C. Walton (Eds.), *Understanding modern warfare* (*2nd* ed., pp. 185–207). Cambridge University Press; Cambridge, United Kingdom.

Kraska, J., & Baker, B. (2014). Emerging Arctic security challenges. Center for New American Security. https://www.files.ethz.ch/isn/178414/CNAS_EmergingArcticSecurityChallenges_policybrief.pdf

Krepon, M. (2008). T*he 1998 Indian and Pakistani Nuclear Test*. Arms Control Association, https://www.armscontrol.org/act/2008-06/looking-back-1998-indian-pakistani-nuclear-tests .

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy*, *38*(11), 1134–1145. doi:10.1016/j.telpol.2014.10.002

Ling, M. F., Moon, T., & Kruzins, E. D. (2005). Proposed network centric warfare metrics: From connectivity to the OODA cycle. *Military Operations Research*, *10*(1), 5–13. doi:10.5711/morj.10.1.5

Lohaus, P. (2015). Special operations forces in the gray zone: An operational framework for using special operations forces in the space between war and peace. *Special Operations Journal*, *2*(2), 75–91. doi:10.1080/23296151.2016.1239989

Manrique, M. (2018). The state of the American mind: 16 leading critics on the new anti-intellectualism. *Literatura: Teoria, Historia, Critica*, *20*(2), 362–369. doi:10.15446/lthc.v20n2.70338

Maras, M. (2017). Overcoming the intelligence-sharing paradox: Improving information sharing through change in organizational culture. *Comparative Strategy*, *36*(3), 187–197. doi:10.1080/01495933.2017.1338477

Margolin, J. and Bruggeman, L. (2021). Months ahead of Capitol riot, DHS threat assessment group was gutted: Officials. ABC News, January 09, 2021. 75155673https://abcnews.go.com/US/months-ahead-capitol-riot-dhs-threat-assessment-group/story?id=

Margolis, G. (2013). The lack of HUMINT: A recurring intelligence problem. *Global Security Studies*, *4*(2), 43–60. http://globalsecuritystudies.com/Margolis%20Intelligence%20%28ag%20edits%29.pdf

Marrewijk, A. (2018). Digging for change: Change and resistance in interorganizational projects in the utilities sector. *Project Management Journal*, *49*(3), 34–45. doi:10.1177//87569728770590

Marrin, S. (2001). Intelligence analysis and decision-making: Methodological challenges. In P. Gill, S. Marrin, & M. Phythian (Eds.), *Intelligence theory: Key questions and debates*. pp. 131-150. London, United Kingdom: Routledge. doi:10.4324/9780203892992.

Mattis, P. (2015). China's New Intelligence War Against the United States. *War On The Rocks*, July 22, 2015. https://warontherocks.com/2015/07/chinas-new-intelligence-war-against-the-united-states/

National Science and Technology Council (NSTC). (2021). National Strategic Overview for Research and Development Infrastructure. Executive Office of the President of the United States. https://www.whitehouse.gov/wp-content/uploads/2021/10/NSTC-NSO-RDI-_REV_FINAL-10-2021.pdf

Ochiai, Y., (2011). US Intelligence and the Origins of the Vietnam War, 1962–1965 [PhD Thesis]. University of Edinburgh.

Odom, W. E. (2001). Intelligence analysis. *Intelligence and National Security*, *23*(3), 316–332. doi:10.1080/026845208021216

Office of the Director of National Intelligence (ODNI). (2017). *Intelligence Community Information Environment (IC IE) Data Strategy* 2017–2021. Office of the Director of National Intelligence. https://www.dni.gov/files/documents/CIO/Data-Strategy_2017-2021_Final.pdf .

Office of the Director of National Intelligence (ODNI). (2019a). *National Intelligence Strategy of the United States of America 2019*. Office of the Director of National Intelligence. https://www.dni.gov/index.php/newsroom/reports-publications/itemlist/category/297-reports-publications-2019 .

Office of the Director of National Intelligence (ODNI). (2019b). *The AIM Initiative: A Strategy for Augmenting Intelligence Using Machines*. Office of the Director of National Intelligence. https://www.dni.gov/files/ODNI/documents/AIM-Strategy.pdf .

Office of the Director of National Intelligence (ODNI). (2020). *National counterintelligence strategy of the United States of America 2020*. Office of the Director of National Intelligence; o, DC, United States of America.

Office of the Director of National Intelligence (ODNI). (2021). *History*. Retrieved January 1, 2021. https://www.dni.gov/index.php/who-we-are/history

Office of the White House. (2013). *National Strategy for the Arctic Region*. https://www.whitehouse.gov/sites/default/files/docs/nat_arctic_strategy.pdf

Office of the White House. (2017). *National Security Strategy of the United States of America*. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf .

Office of the White House. (2018). *Summary of the National Defense Strategy of the United States of America*. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf .

Office of the White House. (2021). *Presidential Memorandum on United States Government-Supported Research and Development National Security Policy*. January 14, 2021. https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/

Pardo Del Val, M., & Fuentes, C. (2003). Resistance to change: A literature review and empirical study. *Management Decision*, *41*(2), 148–155. doi:10.1108/00251740310457597

Paul, C. L. (2008). A modified Delphi approach to a new card sorting methodology. *Journal of Usability Studies*, *4*(1), 7–30.

Peters, B. (2009). Persistence of innovation: Stylized facts and panel data evidence. *Journal of Technology Transfer*, *34*(2), 226–243. doi:10.1007/s10961-007-9072-9

Scheele, D. S. (1975). Reality construction as a product of Delphi interaction. In H. A. Linstone & M. Turoff (Eds.), *The Delphi method: Techniques and applications* (pp. 37–71). Reading, MA: Addison Wesley Publishing Company.

Schmidt, R. C., Lyytinen, K., Keil, M., & Cule, P. (2001). Identifying software project risks: An international Delphi study. *Journal of Management Information Systems*, *17*(4), 5–36. doi:10.1080/07421222.2001.11045662

Shoaib, A. 2021. "China's new hypersonic missile demonstrated an advanced space capability that caught the US intelligence by surprise, report says," Business Insider, https://www.businessinsider.com/chinas-hypersonic-missile-surprised-us-spies-with-its-space-capability-2021-10#:~:text=1%20In%20August%2C%20China%20tested%20a%20hypersonic%20missile,China%20have%20been%20competing%20to%20develop%20hypersonic%20weapons, accessed November 12, 2021

Stimpson, C., & Habeck, M. (2016). *Reforming Intelligence: A Proposal for Reorganizing the Intelligence Community and Improving Analysis*. The Heritage Foundation. https://www.heritage.org/defense/report/reforming-intelligence-proposal-reorganizing-the-intelligence-community-and

Stobierski, T. (2021). Data Wrangling: What It Is & Why It's Important. Harvard Business School Online. Retrieved January 20, 2021. https://online.hbs.edu/blog/post/data-wrangling

Studeman, M. (2007). Strengthening the shield: U.S. Homeland security intelligence. *International Journal of Intelligence and Counterintelligence*, *20*(2007), 195–216. doi:10.1080/08850600601079925

Tatlow, D. (2020). Exclusive: 600 U.S. Groups Linked to Chinese Communist Party Influence Effort with Ambition Beyond Election. Newsweek, October 26, 2020. https://www.newsweek.com/2020/11/13/exclusive-600-us-groups-linked-chinese-communist-party-influence-effort-ambition-beyond-1541624.html

Tingstad, A., Savitz, S., Van Abel, K., Woods, D., Anania, K., Ziegler, M., . . . Costello, K. (2018). *Identifying Potential Gaps in U.S. Coast Guard Arctic Capabilities*. Homeland Security Operational Analysis Center operated by the RAND Corporation. https://www.rand.org/pubs/research_reports/RR2310.html .

U.S.-China Economic and Security Review Commission (USCC). (2016). *2016 Report to Congress of the U.S.-China Economic and Security Review Commission*, November 2016, Section 3, 289–304.

U.S.-China Economic and Security Review Commission (USCC). (2020). *2020 Report to Congress of the U.S.-China Economic and Security Review Commission*, December 2020. https://www.uscc.gov/sites/default/files/2020-12/2020_Annual_Report_to_Congress.pdf

Ucko, D., & Marks, T. (2018). Violence in context: Mapping the strategies and operational art of irregular warfare". *Contemporary Security Policy*, *39*(2), 206–233. doi:10.1080/13523260.2018.1432922

United States Geospatial Intelligence Foundation (USGIF). (2020). *Geospatial Intelligence & AI/ML Progress During a Pandemic: How the IC Has Adapted to the Challenges of COVID-19*. November 2020. https://usgif.org/wp-content/uploads/2020/11/Geospatial_Intelligence_and_AI-ML_Progress_During_a_Pandemic_FINAL-1.pdf

Vance, C. (2018). *The Future of US Intelligence: Challenges and Opportunities*. NATO Association of Canada/Association Canadienne Pour L'OTAN, Emerging Security. http://natoassociation.ca/the-future-of-us-intelligence-challenges-and-opportunities/

Voelz, G. (2006). *Managing the Private Spies: Use of Commercial Augmentation for Intelligence Operations* (Discussion Paper #14). Joint Military Intelligence College.

Votel, J., Cleveland, C., Connett, C., & Irwin, W. (2016). Unconventional warfare in the gray zone. *Joint Forces Quarterly*, *80*(2016), 101–109. http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-80/jfq-80_101-109_Votel-et-al.pdf

Wardlaw, G. (2015). Is the intelligence community changing appropriately to meet the challenges of the new security environment? In G. Bammer (Ed.), *Change! Combining analytic approaches with street wisdom* Canberra, Australia: ANU Press, The Australian National University. published 2015 by, Chapter 8, pp. 107-128. http://press-files.anu.edu.au/downloads/press/p319221/pdf/ch082.pdf

Wasserman, L. (2018). Topological data analysis. *Annual Review of Statistics and Its Application*, *5*(2018), 501–532. doi:10.1146/annurev-statistics-031017-100045

Williams, P., Alessa, L., Kliskey, A., Rinella, D., Trammell, J., Powell, J., … Abatzoglou, J. (2018). The role of perceptions versus instrumented data of environmental change in decision-making: Implications for increasing adaptive capacity. *Environmental Science & Policy*, *90*(2018), 110–121. doi:10.1016/j.envsci.2018.09.018

Yanalitis, M. (2014). *Red Teaming Approach Rationale and Risks*. https://www.researchgate.net/publication/259546738_Red_Teaming_Approach_Rationale_and_Risks

Young, A. (2019). *Too Much Information: Ineffective Intelligence Collection*. Harvard International Review (August 2019). https://hir.harvard.edu/too-much-information/ .

Zimmermann, M. and Eguíluz, V. (2005). Cooperation, social networks, and the emergence of leadership in a prisoner's dilemma with adaptive local interactions. Physical review. E, Statistical, nonlinear, and soft matter physics, 72 (Dec), 056118, doi:10.1103/PhysRevE.72.056118