ON THE RADAR

KEY TAKEAWAYS FROM

UNDER THE NUCLEAR SHADOW

Situational Awareness Technology and Crisis Decisionmaking

AUTHORS

Rebecca Hersman, Reja Younis, Bryce Farabaugh, Bethany Goldblum, Andrew Reddie

Improvements to strategic situational awareness (SA)—the ability to characterize the operating environment, detect and respond to threats, and discern actual attacks from false alarms across the spectrum of conflict—have long been assumed to reduce the risk of conflict and help manage crises more successfully when they occur. However, with the development of increasingly capable strategic SA-related technology, growing comingling of conventional and nuclear SA requirements and capabilities, and the increasing risk of conventional conflict between nuclear-armed adversaries, this may no longer be the case.

"Information dominance has been essential to ensuring U.S. military effectiveness, sustaining the credibility and assurance of military alliances, and stabilizing or reducing the risks of miscalculation or collateral damage. But can there be too much of a good thing?"

-From *Under the Nuclear Shadow* Full Report

CENTRAL QUESTIONS

1. What is the strategic SA ecosystem and how has it evolved?
2. Which technical capabilities will inform strategic SA in crisis and conflict between nuclear-armed adversaries?
3. How can these capabilities decrease or increase escalatory risks in crises that occur under a nuclear shadow?

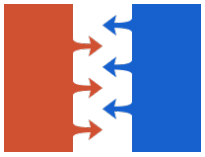
***With the support of the Carnegie Corporation of New York**, the Project on Nuclear Issues (PONI) at the Center for Strategic and International Studies (CSIS) and the University of California, Berkeley's Nuclear Policy Working Group undertook a two year study to examine the implications of emerging situational awareness technologies for managing crises between nuclear armed adversaries. This visual booklet provides an overview of key concepts, conclusions, and recommendations from our study on the impact of emerging technologies for situational awareness on strategic stability. The full report can be found at* **ontheradar.csis.org**

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

What Is the Evolving Strategic Situational Awareness Ecosystem?

CONVENTIONAL
Capabilities that provide theater and battlefield-level situational awareness, to include related indications, warning or other operational information as well as information on the status, location, and condition of conventional assets and capabilities.

NUCLEAR
Capabilities that provide indications, warning or other operational information on the status, location, or condition of adversary nuclear weapons, delivery or command and control systems.



TRADITIONAL
(approx. 1950-1990)

Nuclear and conventional SA ecosystems operated mostly independently, with largely passive, secure, and compartmentalized assets that operated outside of adversary territory and beyond range of attack.

TRANSITIONAL
(approx. 1990-2020)

Technological development (2nd Offset) in conventional SA assets vastly outpaces innovation in nuclear arena. There is growing dependence on nuclear command, control, and communications to support conventional operations.

EMERGING
(2020 Forward)

Increasingly capable SA assets are highly networked and dual-use, with blurred boundaries between conventional and nuclear.

Why Does This Matter?

1. The risk of crisis or conflict between nuclear-armed states—some of which integrate conventional and nuclear forces in their military strategies or employ dual-use (nuclear and conventional) delivery systems—is increasing.

2. Nuclear-armed states are increasingly reliant on a single strategic SA-enabled ecosystem for both nuclear and conventional crisis and conflict, raising new escalation challenges and prompting reconsideration of the value and stabilizing nature of information dominance in a crisis.

3. New technologies provide more information quicker and with greater precision than ever before, challenging decisionmakers' ability to effectively manage risk and adjudicate the high stakes involved.

"The rapid expansion of new and existing technologies can provide opportunities for major breakthroughs in the ability to: detect threats; track hostile actions and forces; process, interpret, and communicate vast data sets; and predict and shape the actions and possibly even decisions of adversaries."

-From *Under the Nuclear Shadow* Full Report

What Are the Attributes and Risk Factors of Emerging SA Technologies?

ATTRIBUTES *FOR INCREASING STRATEGIC SA*

ATTRIBUTES	DEFINITION	TECHNOLOGY EXAMPLES
Vantage/ Range	*The position from which new information can be ascertained.*	*Pseudosatellites that can position highly capable sensors outside of targetable distance.*
Speed	*The shortening of time between an adversary's action or decision to act, detection of that action, and the receipt of such by decision-makers.*	*Quantum computing that accelerates the ability to process and analyze vast data sets.*
(Un)detectability	*The degree to which an adversary can ascertain that information is being collected.*	*Advanced stealth capabilities that allow sensor platforms to evade detection by adversary air defenses.*
Precision	*The level of detail and quality of the information collected or a heightened degree of confidence in the information collected.*	*Synthetic Aperture Radar (SAR) that can track military movements despite weather and cloud cover.*
Smallsat	*The extent to which the capability can continuously collect data without gaps in coverage.*	*SmallSat constellations that can surveil specific areas for weeks or months.*
Resiliency/ Reliability	*The ability of a technology to employ redundant and robust systems for situational awareness in a contested environment.*	*Multi-sensor payload UAV swarms that can operate even if some of the platforms are destroyed or disabled.*

RISK FACTORS *FOR DECREASING STRATEGIC STABILITY*

STABILITY RISK FACTOR	DEFINITION	TECHNOLOGY EXAMPLES
Intrusive	*The extent to which a capability must enter an adversary's territory, airspace, or networks.*	*An autonomous UUV or UAV with advanced sensing capability deployed inside adversary territory, airspace, or waters.*
Destructive	*The extent to which a capability can disable or degrade an adversary system, either temporarily or permanently, in achieving its objective.*	*A cyber exploit that can detect a decision message by an adversary and disrupt or alter the message at the same time.*
Clandestine	*The extent to which capabilities derive significant military advantage by being kept secret and pose significant disadvantage if revealed.*	*Use of covert personnel or capabilities to deploy highly advanced sensing capabilities in adversary territory.*
Vulnerable	*The degree to which an adversary can deny the use of a capability.*	*Air, maritime, or space surveillance assets that are vulnerable to shoot down, spoofing, or blinding.*
Dual-use	*The extent to which a capability is used for conventional and nuclear missions.*	*Space-based surveillance or communications systems that support both conventional and nuclear missions.*
Predictive	*The degree to which a capability allows a state to anticipate adversary actions as opposed to merely reacting to them after they are completed.*	*AI decision support tools that examine patterns of behavior and detect anomalies to improve the accuracy and timeliness of warning.*
Preemptive	*The extent to which a capability enables acting against adversary actions or plans before they can be completed.*	*Air, ground, or sea-based sensors that can detect the movement of mobile missiles prior to launch.*
Action-enabling	*The degree to which a capability enables new military options.*	*Cyber exploit that can identify and (if desired) disable network or space-based capabilities; or unmanned air or maritime surveillance capabilities that can identify and locate adversary capabilities and provide real-time targeting.*

Which Technologies Were Explored During On the Radar?

STRATEGIC SA CAPABILITY	DOMAIN & TYPE	DEFINITION
Autonomous Unmanned Underwater Vehicle (UUV)	P	Sea-based sensor platform with little to no human input
Unmanned Underwater Vehicle UUV) Swarms	P	Groups of UUVs networked together
Unmanned Underwater Vehicle (UUV) Nets	P	UUVs deployed to passively monitor geographic chokepoints
Unmanned Surface Vehicle (USV)	P	Unmanned surface platform capable of being underway for weeks on end
High Altitude Long Endurance (HALE) UAV	P	Unmanned aerial vehicle with wide range of sensor capabilities
High Altitude Pseudosatelites	P	Extremely high-altitude UAVs with lengthened wingspan able to surveil an area of interest for days to weeks
Unmanned Aerial Vehicle (UAV) Swarms	P	Groups of UAVs networked together to surveil targets in close proximity
Unmanned Underwater Vehicle (UUV)-Launched Unmanned Aerial Vehicle (UAV)	P	Small UAV deployed from UUV with limited optical sensors and comms capabilities
Autonomous Unmanned Aerial Vehicle (UAV)	P	Next-generation unmanned aircraft with both reconnaissance and warfighting capabilities
Manned, Next-Gen Stealth Aircraft	P	Next-generation manned stealth aircraft equipped with optical sensors
Smallsat Constellations	P	Small satellites networked together to surveil target
Co-Orbital Reconnaissance Satellites	P	Small satellites placed in a similar orbit to their target
Quantum Computing	P	Computers that take advantage of physics at the quantum level
Artificial Intelligence (AI) Analysis applications	CE	Computer applications to support human analysts and decision-makers
Cyber Surveillance	CE	Software and hardware that provides access to an adversary's computer network
Compact, Multisensor Proximity Devices	CE	Credit-card sized secure, low-resolution wireless sensors
Plant-based Sensors	CE	Physiology-based sensors capable of reporting the presence of various stimuli
Light Detection and Ranging (LIDAR)	CE	A sensor that generates spatial data from light reflected from a laser
Hyperspectral Sensors	CE	Takes hundreds or thousands of contiguous images in narrow wavebands
Non-acoustic Submarine Detection	CE	Detection technologies including light-based imaging and magnetic detection
Remote Radiation Detection by Electromagnetic Air Breakdown	CE	Uses the reflection of high-intensity pulses to probe the concentration of charged species produced by ionization in air
Electro-Optical (EO) Sensor	CE	Use lenses and mirrors to image objects across the electromagnetic spectrum
Gravity Gradiometer	CE	Passive sensor that measures minute differences in the earth's density
Synthetic Aperture Radar (SAR)	CE	Radar-based sensor used to build high-resolution imagery from mobile platforms
Inverse Synthetic Aperture Radar (ISAR)	CE	Uses movement of the target to generate high-resolution images
Cognitive Electronic warfare		Uses AI to enhance development and operation of electronic warfare technologies
Spoofing		Cyber attack in which attacker masquerades as legitimate user and provides false data to the system
Satellite jamming		Electronic anti-satellite (ASAT) attack that interferes with communications traveling to and from a satellite (downlink and uplink)

SEA AIR LAND SPACE CYBER DEFENSE/COUNTERING P = PLATFORM CE = CRITICAL ENABLER

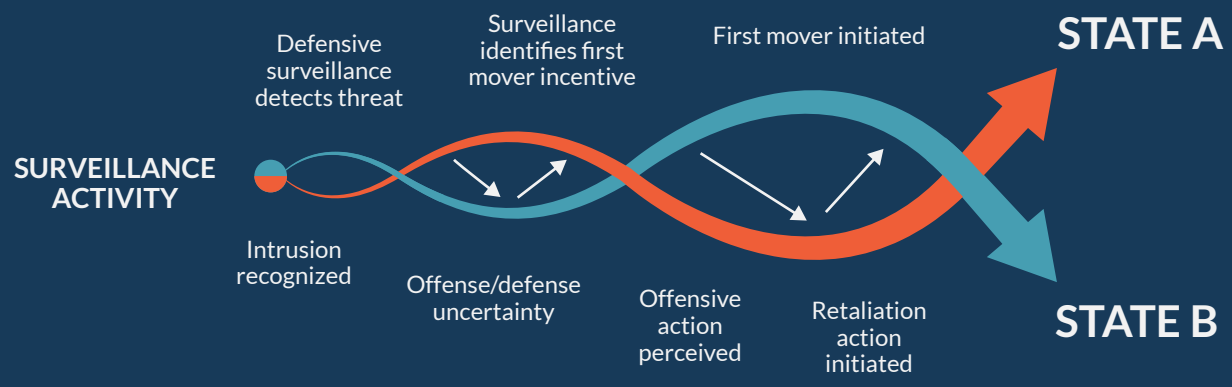
EXAMPLE OF STRATEGIC SA APPLICATION	DEMONSTRATIVE TECHNOLOGY	DOMINANT ATTRIBUTES	DOMINANT RISK FACTORS
Employed to track submarine and surface vessels	Large Diameter UUV (LDUUV)	Vantage/ Range, Persistence	Intrusive, Preemptive
Swarms to specific submarine or surface vessel target (including ports)	Aquabotix UUV Swarm	Persistence, Resiliency/ Reliability	Intrusive, Action-enabling
Static/slow-moving UUVs deployed to littoral waters/geographical chokepoints to track submarineand surface vessel activity		Persistence, Precision	Preemptive, Clandestine
Used to patrol, track, and deploy a range of smaller USV and UUV systems	U.S. Navy Autonomous Swarmboats; Aquabotix USV Swarm	Vantage/ Range, Precision	Intrusive, Vulnerable
Surveil adversary capabilities at high-altitude and maneuverable to lower altitudes	RQ-4, RQ-180	Vantage/ Range, Precision	Intrusive, Vulnerable
Provides long-term, persistent coverage of land and surface targets from over 65k feet in altitude	Airbus Zephyr; Boeing PhantomEye	Vantage/ Range, Persistence	Intrusive, Vulnerable
Deployed to surveil land and sea targets at short distance	DARPA Gremlins Program	Vantage/ Range, Resiliency/ Reliability	Intrusive, Action-enabling
Designed to take aerial images of coastal targets in close proximity		Speed, Precision	Intrusive, Preemptive
Provides aerial imaging and real-time reconnaissance over land and sea targets	Predator MQ-1, MQ-9, MQ-X	Vantage/ Range, Precision	Intrusive, Vulnerable, Dual-use
Performs high-altitude reconnaissance missions of and and sea targets	Lockheed TR-X	Speed, (Un)detectability	Intrusive, Dual-use
Employs advanced sensors from space to surveil targets	SensorSat	Persistence, Resiliency/ Reliability	Preemptive, Dual-use
Tracks and monitors space-based adversary capabilities including satellites used for surveillance, communications, and early warning		Vantage/ Range, Persistence	Dual-use, Clandestine
Enables increasingly rapid data analysis as well as processing power for increasingly autonomous systems	China's National Laboratory for Quantum Information Science	Speed, (Un)detectability	Predictive, Action-enabling
Reconciles diverse data streams to rapidly provide pattern recognition and anomaly detection tools to analysts	Project Maven	Speed, Precision	Predictive, Vulnerable
Provides insight into adversary behavior, intentions, and decision-making	Eternal Synergy and Double Pulsar	(Un)detectability, Persistence	Intrusive, Clandestine
Passive sensors placed close to land target location. Example target includes nuclear fuel fabrication facilities		Precision, Persistence	Intrusive, Clandestine
Employed in adversary territory to monitor for certain chemical or radiological signatures associated with activities of interest	DARPA Advanced Plant Technologies Program	Vantage/ Range, (Un)detectability	Intrusive, Clandestine
Rapidly 3D maps a target area from air, space, or the surface of the ocean with potential tracking capabilities	DARPA HALOE	Precision, Persistence	Dual-use, Preemptive
Provides a picture of adversary behavior using hyperspectral images that cut through obstacles to optical sensors	ACES-Hy UAV sensor	Vantage/ Range, Precision	Dual-use, Preemptive
Magnetometers, in particular, are used to attempt to track adversary submarines	China's Guanlon Project	Vantage/ Range, Precision	Clandestine, Action-enabling
Used to detect nuclear activity in facilities across the fuel cycle.		Vantage/ Range, Precision	Intrusive, Preemptive
Used to detect and track aircraft, missile launch warning, target acquisition and surveillance, etc.	ARGUS	Vantage/ Range, Precision	Dual-use, Preemptive
Yields information on geologic structures underground and undersea used to surveil tunneling by adversaries		Vantage/ Range, Precision	Dual-use, Preemptive
Used to surveil and detect land-based assets such as mobile missiles	RADARSAT-2	Precision	Dual-use, Preemptive
Able to image moving objects from a variety of vantage points		Precision	Dual-use, Preemptive
Used in attempt to detect, suppress, and neutralize cyber attacks		Speed, Persistence	Predictive, Clandestine, Destructive
Can be used to take control of a satellite or inject corrupt data into communications or otherwise poison data from SA sources		Vantage/ Range, Precision	Intrusive, Action-enabling, Destructive
Can be used to disrupt missile warning systems, SIGINT, GPS, and communications satellites	Krasukha-2, Zhitel, and Borisglobesk	Persistence, Resiliency/ Reliability	Action-enabling, Destructive

How Could These Capabilities Contribute to Escalation?

Of particular concern are three potential escalation pathways—provocation, entanglement, and information complexity—that may be triggered or exacerbated with the use of emerging strategic SA-enhancing capabilities. During an actual crisis, multiple pathways may be activated, either simultaneously or sequentially. Examining each of these escalatory pathways individually provides insight into the interplay of strategic SA technologies and stability risks.

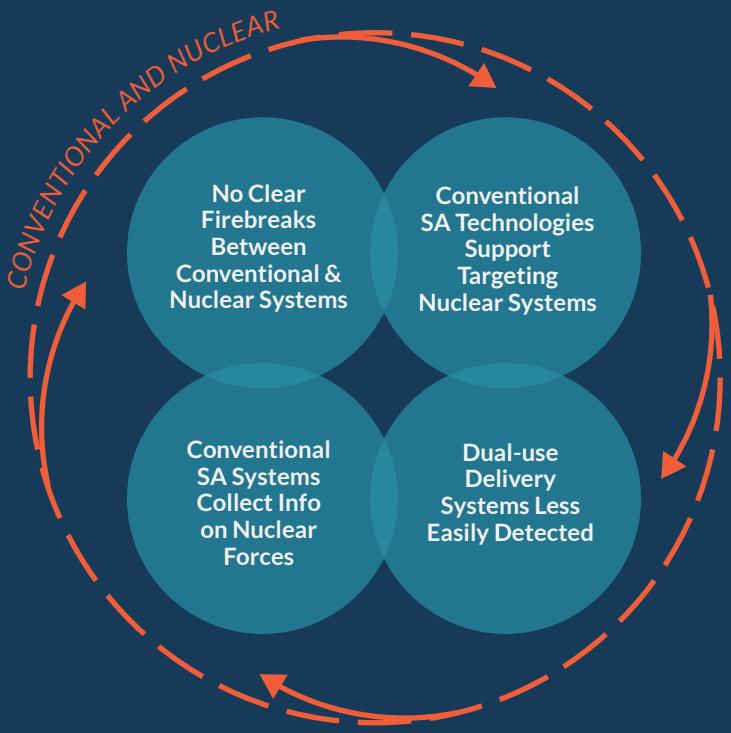
PROVOCATION

Decisionmakers' perception of information collection as either offensive or incentivizing an offensive advantage



ENTANGLEMENT

Decisionmakers' inability to delineate between nuclear and conventional risks

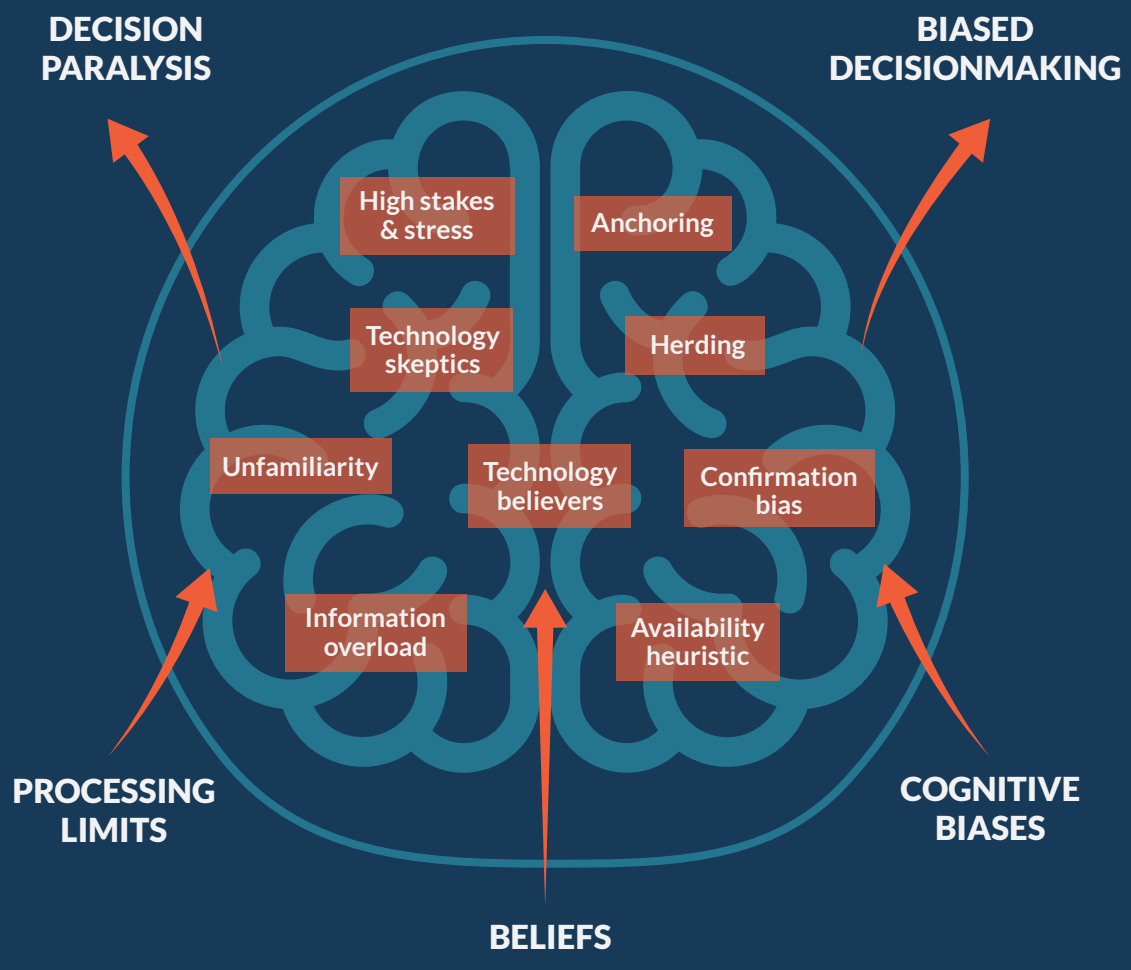


"Psychology, particularly in the form of pre-existing beliefs and cognitive biases, is underappreciated when examining the relationship between crisis decisionmaking and emerging technology."

-From *Under the Nuclear Shadow* Full Report

INFORMATION COMPLEXITY

Decisionmakers' inability to seek, manage, and interpret information effectively



8 TABLETOP EXERCISES

The project ran a series of tabletop exercises to better understand how policymakers evaluate risks associated with employing emerging technologies to enhance situational awareness during crises between nuclear-armed adversaries.

By the Numbers

HELD IN

5 locations across **4** different states

APPROXIMATELY

150 participants, including next-generation scholars, mid-career professionals, and senior experts

40+ Hours of Discussion

> ***"Policymakers were highly attuned to the escalatory risk associated with intrusive technologies, often weighing their concerns about the potential provocational risks to be more important than the situational awareness benefit that capabilities may provide."***
>
> -From *Under the Nuclear Shadow* Full Report

Blind Spot

In the year 2024, tensions run high as a close-approach incident between the Chinese and Taiwanese navies in the Taiwan Strait sets off a crisis. The United States reaffirms its commitment to defending Taiwan against Chinese aggression as concerns rise over a flash invasion. Complicated by the introduction of grey-zone tactics like satellite "dazzling" and GPS spoofing that significantly limit American visibility in the region, the situation threatens to escalate a regional crisis into a full-blown conflict between near-peer adversaries.

Risky Business

In the year 2025, a crisis unfolds as North Korea takes provocative actions against South Korea, including seizing an island, taking South Korean soldiers hostage, and ultimately establishing a forward position 20 KM south of the Demilitarized Zone. United States forces on the peninsula are on high-alert as North Korean intentions are unclear and intelligence indicates growing North Korean confidence in their nuclear deterrent. With American troop reinforcements 30 days away, the situation threatens to escalate an inter-Korean dispute into a conflict between two asymmetric nuclear powers.

The Way Ahead

In any crisis between nuclear powers, the nuclear shadow will loom large. This environment will require new perspectives on the value and risks associated with information dominance and its impact on nuclear crises. To effectively manage crisis escalation, decisionmakers must understand how the strategic SA ecosystem has evolved, appreciate the dynamic relationship between improved strategic SA and crisis stability, and recognize the complex interplay between technology, escalation, and decisionmaking.

The growing nuclear shadow requires new perspectives on the value and achievability of information dominance.

As the risk of crisis between nuclear-armed adversaries increases, assumptions about the value and achievability of information dominance may need to be reconsidered. Information dominance has been essential to ensuring U.S. military effectiveness, sustaining the credibility and assurance of military alliances, and stabilizing or reducing the risks of miscalculation or collateral damage, especially in post-cold war conventional conflicts. In the combined conventional-nuclear strategic SA ecosystem, surveillance capabilities vital to U.S. conventional superiority may introduce underappreciated escalatory risks and anxieties. Careful reexamination is required.

The risk of inadvertent escalation will dominate how decisionmakers think about a crisis between nuclear-armed states. The presence of new technologies can enhance situational awareness and influence risk perceptions, both positively and negatively. New technologies can provide more information more quickly and with greater precision than ever before, but decisionmakers must weigh the benefits of more rapid, decisive military victory afforded by information dominance against the high-stakes risks of possible nuclear escalation. Escalation anxiety may make decisionmakers assess the value of information and the means of its collection differently and with greater caution.

Critical decisions necessary to achieve and manage information dominance will occur early in a crisis as both sides seek to understand and resolve the crisis on the most favorable terms possible. Effective tools to evaluate risk, utility, and confidence associated with strategic SA capabilities are lacking, especially early in a crisis when the situation is most uncertain and information demands are high.

Despite the potential value of enhanced SA, decisionmakers may reject certain capabilities during a crisis if they perceive them as provocative or escalatory. Escalation aversion could result in information gaps during a crisis, contributing to strategic surprise, deterrence failure, or miscalculation. This could create new, unanticipated paths toward escalation or alternatively lead decisionmakers to "micromanage" their use. This could exacerbate tensions between policymakers and operators, whose needs and perspectives on the value of supplemental information may differ.

The combined conventional/nuclear strategic SA ecosystem is here to stay.

Comingled platforms, mutual dependencies between conventional and non-conventional capabilities, and the need for strategic SA capabilities to address nuclear risks preclude relying on "disentanglement" as a primary means of risk reduction. Many technologies (e.g., artificial intelligence, advanced sensors, autonomous unmanned platforms) will be comingled and integrated on single platforms, as well as interchangeable across platforms, requiring new frameworks and lexicons to understand the potential strategic risks and benefits of using them. Nuclear and conventional missions will be distinguished less by the capabilities used and more by the missions to which they are assigned.

The strategic SA ecosystem may be combined across the conventional and nuclear realms, but the communities responsible for planning, policy, and crisis management in these two operational areas are not. That needs to change. Communication and collaboration across both communities is essential to understand trade-offs, risks, and benefits to conventional-nuclear integration in the strategic SA arena.

Nuclear and conventional communities—military and civilian—bring different perspectives, familiarity, and comfort with different technical capabilities and in turn will raise different questions and maintain different assumptions about the risks and benefits of their use. Managing conventional crisis under a nuclear shadow will require an appreciation for these differences and a combined approach.

The combined nuclear/conventional strategic SA ecosystem will shape, not just inform, crises with nuclear-armed states.

"The capabilities designed to provide situational awareness and support senior decisionmaking in crisis and conflict are increasingly comingled into a single conventional/nuclear ecosystem."

-From *Under the Nuclear Shadow* Full Report

Strategic SA capabilities, especially when used overtly, can signal U.S. intent to an adversary, predict adversary action, manage allies and partners, and shape the international environment more broadly. On the other hand, tactical or operational collection decisions—such as where unmanned aircraft can fly or which cyber systems will be penetrated—will be infused with strategic meaning and consequences.

The United States will need to weigh when, whether, and how to share information regarding the use of new strategic SA technologies with allies and partners in a crisis. This will include questions regarding the disclosure of covert or clandestine capabilities, operational coordination, and "rules of the road" in terms of friend-on friend-surveillance.

To improve their utility in a crisis, autonomous collection platforms (e.g., unmanned systems, cyber, and space-based systems) must be able to adapt to various policy-imposed limits. Intrusive or clandestine capabilities are most likely to be subject to policy constraints or "guardrails" to limit where, when, or how such capabilities can be used or to establish specific high-level approval processes. At a minimum, collectors and operators must be prepared for additional transparency and disclosure requirements, and policymakers need a clear understanding of the costs, as well as benefits, associated with such constraints.

High stakes and unfamiliar technologies may increase the risk of biased decisionmaking.

"Decisionmakers must understand how the strategic SA ecosystem has evolved, appreciate the dynamic relationship between improved strategic SA and crisis stability, and recognize the complex interplay between technology, escalation, and decision-making."

-From *Under the Nuclear Shadow* Full Report

Cognitive bias—a looming challenge for all decisionmakers—may be exacerbated in the emerging strategic SA ecosystem with unfamiliar technology and high-stakes, high-stress circumstances. Training and preparation can reduce the influence of cognitive biases and improve the decision process regarding the use of information collection capabilities in a crisis, but only if done in advance.

Decisionmakers have few tools to understand how nuclear-armed adversaries perceive the new strategic SA environment, technologies, and their linkages with escalation and risk. As a result, decisionmakers are forced to make assumptions—assumptions an adversary might not share. In the absence of data, decisionmakers look for definable boundaries (e.g., international borders) that may reflect Western values and biases. Filling these gaps should be a priority for future research and a topic for dialogue with both allies and potential adversaries.

The vulnerabilities of some technical capabilities to interference, manipulation, disinformation, spoofing, or even cooptation by an adversary are not well understood, especially in the areas of cyber, space, and artificial intelligence. Under such high-stakes scenarios, decisionmakers will demand high confidence in informational provenance and chain of custody.

How emerging strategic SA technologies are used in peacetime, or in early crises, will have significant bearing on decisionmakers' perspectives and familiarity regarding their acceptable use in crisis and war. Introducing new or unfamiliar capabilities in crisis will prompt additional scrutiny for utility and escalatory risk. Finding ways to utilize these capabilities to enhance strategic SA before a crisis will improve familiarity and may reduce perceived escalatory risks.

Recommendations

Close the divide between technology and policy regarding the benefits, risks, and requirements for strategic SA capabilities. Information complexity and a lack of familiarity with strategic SA capabilities introduces underappreciated risks, especially in high-stakes, high-stress scenarios under a nuclear shadow. Technical, operational, and policy communities lack common views on the utility of some capabilities, the risks of disclosure, and the provocation involved in their use, as well as their vulnerability to tampering or manipulation. Socializing technical capabilities and operational requirements now- through training, exercises, and simulations as well as day to day use for strategic SA- is essential to reducing information risks, minimizing cognitive biases, and improving crisis management.

Integrate strategy, planning, and operations between the conventional and nuclear communities to better prepare for conventional crises under a nuclear shadow. These integrated approaches must incorporate early crisis scenarios and recognize the combined strategic SA ecosystem that supports both nuclear and conventional missions. Differing perspectives on information dominance, escalation anxiety, and transparency need to be appreciated and adjudicated in advance.

Engage with allies and potential adversaries on issues of technology, information, and warning to better understand thresholds, risks, and perceptions in early crisis. The "information space" is underappreciated and critical for understanding and managing crises not only in terms of internal decisionmaking but also externally with partners and potential adversaries. Multilateral planning and exercises with allies and partners should incorporate informational aspects of early crisis management. Similarly, issues of escalatory risks associated with warning, surveillance, and information should be addressed through security and stability dialogues with potential adversaries.

Seek ways to make strategic SA capabilities and the information they provide more adaptable and flexible to potential requirements for enhanced transparency, signaling, self-attribution, information sharing, and public disclosures. This may include the development of mechanisms, protocols, and options needed to manage collection assets beyond traditional covert, clandestine, or intelligence-oriented concepts of operation when needed for signaling and crisis management purposes in a crisis with a nuclear-armed adversary.

ACKNOWLEDGMENTS

This report is the culmination of a two-year study by the Project on Nuclear Issues (PONI) at CSIS and the Nuclear Policy Working Group (NPWG) at the University of California, Berkeley on the emerging strategic SA environment and its impact on nuclear crises. The research team hopes that this report's findings and analysis can inform the policy, military, and technical communities in the United States to better equip decisionmakers in crises.

We want to express our deepest gratitude to **Bernadette Stadler**, for her research work and management of this project from the outset and wish her the best in her graduate studies. A special thank you to those who conducted research for this project along the way: **Alex Lenser, Lizamaria Arias**, and **Shannon Kearney**. We would like to thank our consultants, **Kate Charlet, Jared Dunnmon, Michael Horowitz, Elsa Kania, Philip Reiner, Jason Arterburn,** and **Paul Scharre**, each of whom went above and beyond to help us understand key aspects of this complex issue set.

We relied on the expertise of many other CSIS colleagues, including **Eric Brewer, Maxwell Simon, Rhys McCormick, Kaitlyn Johnson,** and **Lindsey Sheppard**, for their research insights. **Rebecka Shirazi** and **Jeeah Lee** did an outstanding job managing the publication process. We are thankful to have collaborated with the creative members of the Andreas C. Dracopoulos iDeas Lab team: **Emily Tiemeyer** for graphic design; **Jacqueline Schrag** and **Tucker Harris** for construction and design of our microsite; and **Mark Donaldson** and **Christopher Burns** for producing videos used in our tabletop exercises. Over 150 next-generation scholars, mid-career professionals, and senior experts participated in our tabletop exercises, providing insights that shaped this study's research findings and recommendations. Both CSIS PONI Nuclear Scholars and members of the Nuclear Policy Working Group at the University of California, Berkeley, contributed extensively to the writing of technology and country primers on the website.

The authors alone are responsible for the report's findings and recommendations, as well as any errors in fact, analysis, or omission. This report is made possible by support from the Carnegie Corporation of New York.

ABOUT THE AUTHORS

Rebecca Hersman is the director of the Project on Nuclear Issues and senior adviser for the International Security Program at the Center for Strategic and International Studies.

Reja Younis is a program manager and research associate with the Project on Nuclear Issues at the Center for Strategic and International Studies.

Bryce Farabaugh is a research intern with the Project on Nuclear Issues at the Center for Strategic and International Studies.

Dr. Andrew W. Reddie is a postdoctoral fellow at the University of California, Berkeley.

Dr. Bethany Goldblum is a research engineer in the Department of Nuclear Engineering at the University of California, Berkeley.

ABOUT PONI

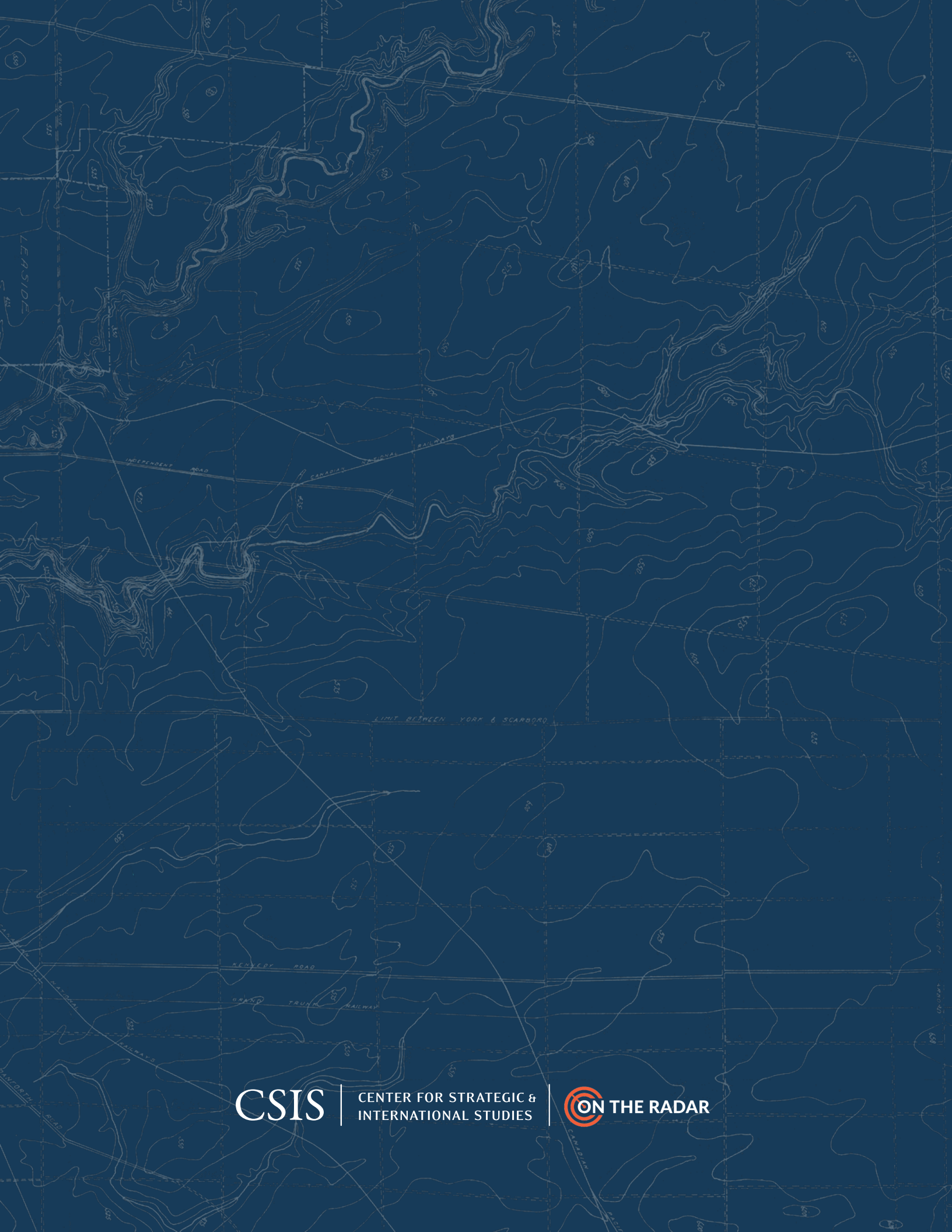
Founded in 2003, PONI is the premier networked community of next generation professionals prepared to meet the nuclear challenges of the future. PONI identifies and cultivates emerging thought leaders by building relationships, deepening understanding and sharing perspectives across the full range of nuclear issues and communities. PONI's programs provide inclusive, diverse, and creative opportunities for emerging experts to learn about policy, technical, and operational aspects of the nuclear enterprise, develop and present new concepts and ideas, engage in thoughtful and informed debates, and opportunities to tour and visit sites across the nuclear enterprise.

ABOUT CSIS

Established in Washington, D.C. nearly 60 years ago, the Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas that address the world's greatest challenges. CSIS is ranked the number one think tank in the United States by the University of Pennsylvania's annual think tank report. To learn more about CSIS, visit www.CSIS.org.

For more research, visit
ontheradar.csis.org

Follow us on Twitter
@csisponi


CSIS
CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES
ON THE RADAR