Naval War College Review

Volume 66
Number 4 *Autumn*

Article 7

2013

Maritime Deception and Concealment: Concepts for Defeating Wide-Area Oceanic Surveillance-Reconnaissance-Strike Networks

Jonathan F. Solomon

MARITIME DECEPTION AND CONCEALMENT

Concepts for Defeating Wide-Area Oceanic Surveillance-Reconnaissance-Strike Networks

Jonathan F. Solomon

The post–Cold War interlude during which U.S. maritime access to and within overseas regions of grand-strategic importance faced few challenges was a historical anomaly. Accordingly, in January 2012 the Department of Defense (DoD) formally recognized in its *Joint Operational Access Concept* (JOAC) document that this pause is ending and that joint capability requirements must be revisited. The JOAC establishes benchmarks for developing the doctrine, training priorities, warfare systems and matériel, organizational structures, and other measures necessary to overcome advanced maritime-denial capabilities across all warfare domains.[1] Woven throughout the JOAC is the need to disrupt or neutralize the theater-wide surveillance and reconnaissance networks that strategic competitors are developing to provide their maritime-denial forces with tactically actionable targeting cues. Indeed, China's and (to a much lesser extent) Iran's deployments of dense, layered, and networked capabilities over the past decade represent continuity with the millennia-old struggles between offense and defense, as well as between localized area control and denial.

The JOAC specifically states that efforts to disable such networks in war require not only kinetic means but also deception and concealment. This is partly because the survivability and deterrence effect of forces deployed forward in a crisis depend in large part on their ability to avoid being targeted.[2] It follows that because standing peacetime rules of engagement constrain prehostilities antinetwork measures,

Mr. Solomon is a senior systems and technology analyst for Systems Planning and Analysis, Inc., in Washington, D.C. He previously served as a U.S. Navy Surface Warfare Officer. This article expands on elements of his April 2011 master's thesis for Georgetown University's Security Studies Program.

Naval War College Review, Autumn 2013, Vol. 66, No. 4

Naval War College Review, Vol. 66 [2013], No. 4, Art. 7

force-level deception and concealment where practicable will be crucial to joint countersurveillance and countertargeting.[3]

Should deterrence fail, physical neutralization of maritime surveillance and reconnaissance sensors, communications pathways, and data-fusion centers would likely consume considerable resources and time.[4] In the meantime, political objectives would likely assign forward maritime forces other tasks that necessarily expose them to the still-capable network.[5] Some network elements are likely to be shielded through hardening, mobility, or positioning beyond strike range. Antinetwork operations may also face self-imposed political constraints stemming from escalation concerns. The network may additionally maintain a "war reserve" to replace neutralized assets and compromised pathways, though returns may diminish as a conflict's duration increases. Nevertheless, the 1991 Gulf War campaign against Iraq's integrated air-defense system suggests that the risks an adversary's network poses would not decrease quickly and could never be completely eliminated via neutralization of nodes and pathways alone.[6]

Deception and concealment can help mitigate these risks—namely, that a network-empowered adversary might cripple U.S. forward maritime forces in a massive, war-opening strike; achieve in the first days or weeks some fait accompli that maritime forces are striving to prevent; or inflict severe losses on maritime forces as they maneuver within the contested zone to retake the initiative. Deception and concealment are hardly new to electronic-age maritime warfare, and although the tactics and historical examples that follow are hardly comprehensive, they help outline potential countersurveillance and countertargeting tools.

Deception and concealment alone cannot guarantee success; they are complements to, rather than substitutes for, robust kinetic weapon systems that physically attrite sensors, weapons, platforms, and network infrastructures. All the same, their absence would likely handicap U.S. forward maritime operations within emerging threat environments, which in turn would impact contemporary conventional deterrence credibility.

MARITIME CONCEALMENT DOCTRINE AND BASIC TACTICS

U.S. joint doctrine defines "concealment" as "protection from observation or surveillance." Concealment is primarily a tactical-level effort that supports deception by "manipulating the appearance or obscuring the deceiver's actual activities."[7] Although some concealment tactics can be used effectively in the absence of deception (defined below), most attain peak effectiveness in tandem with it. In the JOAC framework, concealment falls under the term "stealth."[8]

The most commonly practiced maritime concealment tactic is *emission control* (EMCON). Maritime forces typically restrict their radio-frequency (RF)

emissions and configure shipboard systems to limit acoustic emissions when operating in contested areas; platforms tasked with active sensor searches in support of forces in EMCON are positioned so that the former's emissions do not reveal the latter's general location.[9] As repeatedly demonstrated by the U.S. Navy against the Soviet Ocean Surveillance System (SOSS) during the Cold War, EMCON measures can severely constrain if not eliminate the usefulness of wide-area passive sonar and RF direction-finding or electronic intelligence (ELINT) sensors for surveillance and reconnaissance.[10] EMCON does not necessarily imply complete silence; highly directional line-of-sight communications systems and difficult-to-intercept "middleman" relays (satellites or aircraft) can provide critical command and coordination links. Even so, it does represent a deep cut to the force's normally available bandwidth. Effective EMCON therefore requires decentralized doctrine that embraces unit-level initiative in executing the force commander's intentions, as well as preplanned and frequently practiced responses to foreseeable situations.[11]

Force-level maneuver enables concealment as well. If the adversary's maritime reconnaissance patterns and tactics, surveillance-satellite orbits, fixed-location sensor emplacements, and effective sensor coverages are known with reasonable confidence, ocean transit plans can be designed to reduce the probability of detection or sustained tracking. For example, a force can maneuver to reduce electromagnetic and acoustic exposure.[12] Force-level maneuvers might also be ordered in response to long-range detection of adversary reconnaissance assets or seemingly neutral shipping or aircraft, changes in the adversary's satellite dispositions, or emergent tactical intelligence.

Additionally, a force's operations can be adjusted to exploit meteorological phenomena.[13] Sufficiently dense haze and cloud cover reduces vulnerability to infrared (IR) and visual-band electro-optical (EO) sensors. Precipitation similarly reduces EO/IR sensor effectiveness and, depending on wavelength and clutter-rejection capabilities, sometimes radar as well.[14] Atmospheric layering can cause radar emissions to be so refracted as to render nearby surface units and aircraft undetectable. Highly variable diurnal ionospheric conditions can likewise degrade shore-based over-the-horizon-backscatter (OTH-B) radars. Heavy seas, however uncomfortable for crews, increase the background clutter OTH-B radars must sift through, as well as the ambient noise that complicates passive sonar search.

In the absence of exploitable meteorological phenomena, surface units can lay obscurant "clouds" against EO/IR sensors and millimeter-band radars, as well as chaff clouds against centimeter- and decimeter-band radars. Throughout naval history, ships have employed similar methods to shield themselves from

detection, classification, identification, or precision tracking.[15] Obscurants and chaff are detectable, however; an adversary might reasonably assume that a unit of interest lies somewhere behind or beneath such a cloud and that closer reconnaissance is warranted. The adversary may even directly target the cloud in hopes of temporarily incapacitating the concealed unit. Obscurants and chaff are consequently best employed when supported by tactical deception.

Dispersion is another concealment tactic that works best within an overall deception plan. Naval formations, for instance, are often thought of as like a bull's-eye, with rings of defensive aircraft and escorts surrounding high-campaign-value surface units at the center.[16] This is not always the case. Wide-area sea- and land-based sensors, long-range sea- and land-based weapons, and joint tactical data links allow a dispersed force to extend its sensor and weapons coverage over broad areas and its units to support each other even when not in physical proximity. A dispersed force, therefore, may not be as conspicuous as a traditional formation to wide-area sensors. Combined with selective EMCON and deceptive tactics, dispersion can allow a force to blend into background shipping.[17] The tyrannies of time, distance, speed, fuel, and electromagnetic/acoustic-wave propagation represent, however, an important caveat. As the Imperial Japanese Navy demonstrated at the battle of Midway, a force's dispersion must never be so great that its units cannot quickly and effectively mass their capabilities or provide mutual support should deception fail.[18]

Disciplined *operational security* (OPSEC) and *communications security* (COMSEC) can be considered forms of concealment, as they deny information that could negate a deception plan. By restricting the personnel with knowledge of a planned action and minimizing related communications—encrypted where appropriate and sent only over the most secure and trusted pathways—a force can complicate an adversary's intelligence collection.[19] Although COMSEC measures and cyberdefenses support pathway integrity and confidentiality, a force commander may use human couriers or other "out of band" methods to protect critical messages, despite impacts to throughput and timeliness.[20] Generally speaking, robust OPSEC and COMSEC measures mean a force cannot use finely choreographed plans relying on "just-in-time" updates or direct control. Like EMCON, they compel reliance on "command by negation," a doctrine that empowers unit commanders to exercise initiative to carry out the force commander's promulgated intentions.

Electronic warfare (EW) concealment comprises two main tactics. First, RF and acoustic systems can employ *low-probability-of-intercept* (LPI) hardware and waveforms that make them very difficult to detect, analyze, or exploit. An adversary may eventually extract LPI emissions from the ambient environment, though. LPI capability employment must hinge on risk analysis; certain critical

capabilities should be withheld as war reserve and even in combat used only when absolutely necessary.[21]

Electromagnetic *jamming* is the other major EW concealment tactic. RF noise can effectively saturate older or less sophisticated radar receivers, tax modern radar processing enough to make searching less efficient, and disrupt the communication of a remote sensor or data-relay node with a network.[22] Low-power, solid-state IR and visible-band lasers can be used to blind EO/IR sensors, but because solid-state lasing mediums can excite photons only in narrow wavelength blocks, multiple lasers may be necessary to blind a single multispectral or hyperspectral EO/IR system.[23] The greatest limitation of noise jamming is that an adversary can cross-fix the source of the jamming and cue scouts to search nearby for the supported force. This risk can be mitigated somewhat by positioning airborne jammers so as not to compromise the force's location, or by employing deception.

Lastly, "distributed denial of service" (DDOS) and penetrative "disruption/blinding" cyberattacks against nodes of a surveillance-reconnaissance-strike network potentially contribute to maritime concealment. A DDOS attack saturates a targeted web server with data requests in order to disrupt its hosted services and connectivity. However, an adversary can harden a network against DDOS by using pathways with bandwidths well beyond that needed for most services; redundant war-reserve mirrored servers into which those under DDOS bombardment can "fail over"; war-reserve or "out-of-band" network pathways for rerouting; or agile Internet protocol (IP) address/domain blocking. It is also not clear how a sizable sustained DDOS attack can be practicably directed against military networks that are not connected to the public Internet.

Whereas DDOS attacks are "brute force," penetrative cyberattacks that blind networked sensors, disrupt or corrupt network data-relay pathways, or shut down data-fusion infrastructures require a substantial level of tradecraft. Some might involve "logic bombs" covertly inserted prior to a conflict and triggered by remote signal or insider action. Others may involve real-time penetrations, again dependent on prior intelligence collection against, and exploration of, the adversary's network. Much as with DDOS, though, war-reserve network infrastructures and sensors, as well as out-of-band communications pathways, may be able to limit the duration and impact of a penetrative "disruption and blinding" cyberattack.

This is not to say that these cyberattack types are unlikely to be useful in any scenario but to suggest that they may not be the most effective or viable means for nonkinetically handicapping an adversary's networked systems—unless, at least, one knows with some confidence how severely and for how long they could degrade the adversary.

Naval War College Review, Vol. 66 [2013], No. 4, Art. 7

MARITIME DECEPTION DOCTRINE AND BASIC TACTICS

Joint doctrine defines "military deception" as those "actions executed to deliberately mislead" adversary decision makers as to friendly military capabilities, intentions, and operations, "thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission." An adversary's intelligence, surveillance, and reconnaissance networks are the channels for conveying a deceptive "story" and are not themselves the deception targets. Rather, deception is aimed at specific military or political leaders, with the objective of inducing them to make suboptimal decisions by exploiting their known or apparent preconceptions. It follows that *operational* deception is aimed at campaign/operational-level planners and decision makers, while *tactical* deception focuses on the engagement and battle levels.[24] The boundaries separating operational and tactical deception are increasingly blurry in practice, though, since an adversary's theater-range maritime strike assets may be controlled by a commander who bridges the two levels. Operational deception may therefore be necessary to induce surveillance-reconnaissance-strike asset retasking or repositioning within a theater that makes such assets less usable against a supported force.

Maritime deception tactics are generally most effective when several are simultaneously employed so as to address all adversary sensing methods, as well as to establish and legitimize the deception story. Deception is also generally coordinated with concealment tactics, as well as selective physical neutralization of surveillance and scouting assets.[25] Such coordination denies the adversary information that might reveal the charade while allowing the defender to collect disinformation reinforcing the story.

Visual deception tactics include painting schemes and lighting configurations that make a ship appear from a distance to be of a different type or size. Prefabricated structures and deceptive lighting can simulate austere forward operating bases or airstrips. Less common is deceptive alteration of a ship's structure; for example, in World War II, false stacks installed on Allied tankers in Murmansk-bound convoys prevented their easy identification by Luftwaffe bomber crews, and the Royal Navy reconfigured an obsolescent battleship to look like a newer one in order to lure bombers away from a 1942 Malta convoy. Other visual deceptions merely imply the presence of a unit or group, such as the World War II–era "water snowflake" float, which launched an illumination rocket on a preset time delay at night to convince U-boats that a convoy lay just over the horizon.[26] Visual deceptive tactics are likely to be most effective when used against scouts who for safety limit the time they spend near a force, how close they will approach it, or what active-sensor usage they will risk in its proximity; austere scouts, such as those on civilian or commercial platforms, who lack advanced sensors; or

surveillance-reconnaissance systems that are prevented by natural or artificial phenomena from optimally using their sensors.

Deceptive maneuver tactics include use of misleading routes to manipulate a force's "attractiveness" for investigation or attack, or to mislead as to its actual objectives.[27] As the U.S. Navy periodically demonstrated against the SOSS during the Cold War, decoy groups can draw reconnaissance-strike resources away from a main force in EMCON.[28] Units can additionally exploit an opponent's tactical complacency to conceal their movements by taking advantage of the latter's known transit routes and procedures.[29]

Deceptive communications tactics involve the transmission of messages falsifying identities, compositions, locations, intentions, activities, or states of readiness. Since an adversary probably cannot be expected to intercept, identify as significant, decrypt, and analyze a given message in a timely manner, deception tactics often attack the ability to perform traffic-pattern analysis.[30] For example, the Imperial Japanese Navy employed several anti–pattern analysis tactics to conceal the Pearl Harbor Striking Force's November–December 1941 transit toward Pearl Harbor.[31] Alternatively, an adversary's communications-intelligence apparatus can be saturated with "junk" transmissions or contradictory messages. A decoy unit can also simulate another unit's communications while the latter is in EMCON.[32] Forces can even attempt to penetrate an adversary's communications channels and generate false messages that distract, confuse, or redirect his surveillance and reconnaissance.[33]

Deceptive EW and acoustics often involve equipping platforms, expendable decoys, or unmanned vehicles with systems that simulate another unit's RF or acoustic signatures. The aim is to prevent the actual units from being detected, classified, identified, or tracked. During World War II, the Allies periodically used chaff, radar-reflecting balloons and wire cages attached to floats, corner reflectors on small ships, and even false-target generators to convince enemy radars that a major naval force was operating in a given area, so as to attract attack at the wrong place or allow an actual force to break contact.[34] Identification Friend or Foe (IFF) "spoofing" and deceptive jamming of targeting and weapons-guidance sensors are other deceptive EW tactics that debuted in that conflict.[35] Post-1945 technology developments added electronic "blip" enhancement, integrated simulation of RF and acoustic emissions, and expendable offboard decoy technologies.[36] Today, with sufficient intelligence regarding adversary radars' designs and signal-processing techniques, deceptive EW systems can use such emerging technologies as "digital radiofrequency memory" for precision replication, rapid analysis, subtle modulation, and carefully timed directional retransmission of waveforms to trick adversary radars into "detecting" highly realistic contacts in empty space.[37]

Naval War College Review, Vol. 66 [2013], No. 4, Art. 7

Lastly, *cyberspace operations* are a relatively recent addition to the deception portfolio. A commonly hypothesized "crown jewel" tactic uses intelligence collected about the gateways and computing infrastructure of an adversary surveillance-reconnaissance network to execute cyberattacks that manipulate the situational picture it provides decision makers. The technical challenges and uncertainties of sustaining manipulative cyberattacks throughout a war are severe. For that reason, the most frequently used deceptive cyberspace operation may be the "computer network charade" (CNC), which indirectly supports countersurveillance by hijacking the adversary's intelligence-collection activities.[38]

CNC takes advantage of the fact that timely fusion of intelligence into a situational picture is exceptionally difficult, even when aided by data mining and other analytical technologies, since a human generally has to assess each piece of "interesting" information. Once counterintelligence reveals an adversary's intelligence exploitation activities within friendly forces' networks, CNC can feed manipulative information tied to a deception story or worthless information meant to saturate. This can be done using the existing exploited network elements, or alternatively by introducing "honeypots."[39] Massive amounts of such faked material as documents, message traffic, e-mails, chat, or database interactions can be auto-generated and populated with unit identities, locations, times, and even human-looking errors. The material can be either randomized to augment concealment or pattern-formed to reinforce a deception story, as appropriate. A unit can similarly manipulate its network behavior to defeat traffic analysis, or augment the effectiveness of a decoy group by simulating other units or echelons. All this leaves the adversary the task of discriminating false content from any real items he might have collected.[40]

Regardless of CNC method, it can be determined whether or not planted disinformation has been captured by the adversary. The commonalities of CNC with many communication-deception tactics are not coincidental. In fact, civilian mass media, social networks, and e-mail pathways can also be used as disinformation channels in support of forward forces.[41]

THE ADVERSARY'S FIRING DECISION

To understand how maritime deception and concealment tactics can be optimally combined, it is important to understand how an adversary decides how many weapons to launch and how that number impacts an adversary's campaign requirements. The salvo-sizing calculus is based on the probability that the firing platform will be destroyed or break down prior to weapons release; the probability the weapon itself will fail after launch; the size of the area the weapon's guidance sensors must search for the designated target, as compared to their fields of view; the probability that the weapon will detect and lock onto the target;

the probability that it will be able to penetrate anticipated defenses; and the estimated number of weapons that must hit to inflict a desired amount of damage. The lower the cumulative probability of a single weapon's success and the more of them needed to strike the target to inflict the desired damage, the higher the number of weapons that must be fired per salvo.

A firing decision can therefore represent a hefty opportunity cost to the attacker, as the weapons inventory must be managed against requirements needed for the duration of the campaign and as coercive "bargaining chips" for the political-diplomatic endgame. It follows that the more complex a weapon or the more limited the resources the attacker can allocate to its production, the longer its users must wait for replacements. In a prolonged conflict, the effect is magnified if the defender can restore damaged units' most operationally important capabilities faster than the attacker can replenish weapons. All of this means that it may not matter whether cost differentials allow the attacker to procure several times as many offensive weapons as the defender has ships, aircraft, or land-based sites. It also may not matter that the number of offensive weapons available significantly exceeds the number of targets in track. As with all decisions involving a scarcity, the central metric would seem to be the prospective attacker's self-estimated campaign-level opportunity cost of striking at a given point in time.

A prospective attacker might deal with this problem by devoting the majority of the most capable weapons to a conflict's earliest phases, perhaps including a first strike. It is then that an attacker holds the maximum advantage, as its surveillance and reconnaissance capabilities are not yet heavily degraded by countermeasures and counterattacks. The prospective attacker who believes a conflict will be short might be tempted to expend the inventory quickly, given that chances for using it most effectively will decrease rapidly. The campaign-level opportunity cost of classifying targets "by debris" might well be low under these circumstances.

A defender can exploit this situation by sacrificing lower-campaign-value assets to a first strike and its immediate aftermath, and can also attempt to deceive the attacker into wasting inventory against decoys while the defender conceals higher-campaign-value assets.[42] This approach has the bonus of enabling early data collection and analysis against the adversary's surveillance-reconnaissance-strike architecture under combat conditions to identify quickly exploitable vulnerabilities that were not discoverable during peacetime.[43]

However, if the attacker requires that a given weapon be employable throughout a prolonged conflict and that a certain number be preserved for the endgame, the inventory must be either relatively large, quickly replenishable, or used economically.[44] Under these circumstances, an attacker might hesitate to expend a significant portion of the inventory in a given raid if uncertain which—if

Naval War College Review, Vol. 66 [2013], No. 4, Art. 7

any—targets are valid, especially in the aftermath of a successful deception.[45] It is instructive that throughout the Cold War the vaunted Soviet maritime "reconnaissance-strike complex," notwithstanding its wide-area land, sea, air, and space sensors for over-the-horizon missile targeting, was forced by U.S. Navy deception and concealment to depend consistently on visual-range scouts for positive target identification.[46] The physics of contemporary sensor capabilities and limitations does not suggest that the near future will be any different.

As a result, the more a defender can confuse an inventory-husbanding prospective attacker's situational picture by making it impossible to tell from a distance whether a given contact is what it appears to be or whether high-confidence targets in track are actually the most important ones to attack, the more likely that the attacker will hesitate to strike. In fact, the more the defender can tax the adversary's surveillance and reconnaissance resources through physical attrition, deception, and concealment, the better the chances that high-campaign-value forces will escape attention, unless and until their missions compel them to drop cover.[47]

With this appreciation, we can now outline how deception and concealment can help a force survive a first strike with minimal degradation and then quickly rally to slow down, if not defeat, the follow-on offensive. Though these two tasks contain significant tactical similarities, the vast difference in their strategic circumstances means that the first task is far more challenging than the second. The application of doctrine and tactics to form practicable deception and concealment concepts becomes somewhat different for the two tasks.

BLUNTING FIRST STRIKES AND SALVOS

The defender's tactical deception and concealment prior to a first strike, or naval domain "first salvo," aim to prevent or delay effective targeting of forward forces and high-campaign-value units. Should an attack be delivered, the role of deception and concealment is to draw inbound weapons away from actual units.

The success of a first strike generally hinges on an attacker's own use of deception and concealment to enhance surprise.[48] A defender therefore cannot be certain of detecting and recognizing strategic warnings of imminent war, let alone tactical warnings of imminent attack, with enough confidence and rapidity to implement optimal countersurveillance and countertargeting measures. In any case, indication and warning (I&W) is rarely unambiguous. Even should I&W be accepted and hedging actions directed by the leadership, political and psychological factors are likely so to handicap the response that forward forces will not be able to employ fully their deception and concealment options.[49]

The defender's political objectives during a crisis may further complicate the problem, as exemplified by U.S. Sixth Fleet's operations during the 1973 Yom

Kippur War. By presidential direction, the Sixth Fleet was to maintain forward presence at the war zone's immediate periphery; support the transoceanic, airborne, logistical replenishment of Israel; and deter Soviet naval intervention. These tasks meant that the Sixth Fleet could not use space and maneuver to complicate Soviet targeting, and the confined geography of the eastern Mediterranean only worsened the dilemma. "Tattletale" scouts provided the Soviet 5th Eskadra with high-confidence over-the-horizon missile-targeting data by taking station within close visual range of the highest-campaign-value U.S. combatants.[50] With his concealment and deception options foreclosed, the commander of the Sixth Fleet would have faced an unenviable choice had he received possible I&W of a Soviet first salvo: either exercise his authority under American rules of engagement to unleash his own first salvo against the 5th Eskadra and thereby initiate a superpower conflict, with all its associated escalation hazards, or risk his warships by holding back in hope that a risk-averse Kremlin did not want to chance a Soviet-American war.[51]

The Yom Kippur case illustrates the tactical difficulties of prolonged operations within a confined maritime space during a crisis. When geography so greatly simplifies the search problem, a force might be able to avoid localization and identification for hours at best, even if it maximally employs such basic concealment tactics as EMCON. It follows that the proximity of scouts to a force makes the use of jamming or decoys for countersurveillance and countertargeting unsustainable; it might compromise "tricks" prematurely and with little benefit. Jamming might even be unnecessarily provocative, depending on the situation. Postlaunch concealment, however, may still be highly effective against inbound weapons at low relative cost in resources and mission impact.[52] With adequate intelligence, or at least correct assumptions about weapon guidance, postlaunch EW or acoustic deception may likewise help limit the number of successful hits to a campaign-tolerable level. As will be discussed later, a potential adversary's uncertainties regarding a defender's deception and concealment capabilities against an inbound first strike may reinforce deterrence.

The less confined a crisis's maritime space, however, the more deception and concealment can be tactically effective as well as useful for deterrence. This is especially so if the most vulnerable campaign-valuable elements of a conventional deterrent are positioned outside optimal first-strike range, yet close enough to rapidly blunt the adversary's offensive actions and prevent a fait accompli.[53] For example, when at least two aircraft carriers are present in a theater, one should almost always be under way and able to become quickly unlocatable, even in peacetime. If both carriers must be simultaneously in port during a period of tension, one of those ports should either be outside the optimal first-strike range or in a country that the potential adversary would be reluctant to drag into conflict.

Naval War College Review, Vol. 66 [2013], No. 4, Art. 7

These posture adjustments must be made in consultation between the defender and his forward allies, and they ought to be made in peacetime vice during a crisis to mitigate the risk of misperceptions.[54]

Shifting high-campaign-value units beyond a potential adversary's optimal first-strike range is operationally plausible, because initial forward denial operations against a maritime offensive can be waged by submarines; relatively numerous lower-campaign-value warships with offensive armaments disproportionate to their size; land-based air and missile defenses, as well as antiship missiles on friendly-held forward territories and choke points; sea-based missile defenses protecting forward bases and positions; preinserted forward, territorial-defense ground forces; and widespread offensive and defensive mining.[55] These forces can be supported by maritime-denial and logistical aircraft operating from dispersed forward land bases, distant land bases, or over-the-horizon aircraft carriers.

In contrast, the main operational roles of carrier and expeditionary groups following a first strike would arguably be to temporarily secure highly localized areas—that is, achieve "moving bubble" sea control—to support mass movement of reinforcements and matériel into and perhaps within the theater, protect primary economic lines of communication, and maintain sea bases for projecting maritime denial into areas the adversary seeks to control. In many scenarios, these missions would require carrier and expeditionary groups to operate at least initially from the contested zone's periphery.[56] Raids by these groups within the contested zone may also be desirable.[57]

Given these assumptions, carrier and expeditionary groups could mitigate their first-strike vulnerability as a crisis escalates by taking advantage of wide maneuver space to employ such concealment tactics as EMCON, dispersal, weather masking, artificial obscuration, or evasion. These groups could similarly use deceptive visual, maneuver, communications, and CNC tactics to create countersurveillance and countertargeting *ruses*—decoy units or groups, for example.[58] They might also be able to employ certain EW or cyberattack tactics, as allowed within the rules of engagement and as balanced against the likelihood of revealing exploitation methods and perceived exploitable vulnerabilities, and given relative spatial separation from the potential adversary's sensors and firing platforms.

Even if not in geographically confined waters, though, forward surface forces "locked" to a geographic position or required to operate overtly during a crisis would almost certainly not be able to take advantage of pre–first salvo concealment and deception tactics. It follows that combatants executing such missions as sea-based air and missile defense in support of forward forces would be highly exposed.[59] Forward land-based sensors and weapons, however, might be able to compensate for their constrained tactical mobility through rotational dispersion

among austere basing sites, minimized or deceptive communications and emissions, CNC, and countertargeting *displays* (signature-simulating decoy aircraft and equipment).[60]

A defender might support frontline forces by trying to saturate the adversary's maritime targeting picture from the start of a crisis. It is not clear, though, that such an effort would be practicable, let alone sustainable. This degree of deception might require revealing crown-jewel EW and cyberattack tactics along with vulnerability exploits, which would be worthwhile only if the potential crisis-stabilizing benefits outweighed the probable tactical costs.

Nevertheless, forward forces have some cause for optimism. Although pre–first strike rules of engagement would likely bar direct neutralization of potential adversary manned reconnaissance assets, the same might not be true regarding unmanned ones. There are recent historical precedents of one state neutralizing another's unescorted, unmanned scouts during times of elevated tension without inciting much more than diplomatic protests.[61] Far less stigma attaches to killing robots than manned platforms. A defender might declare exclusion areas during a crisis within which any detected unmanned system would be neutralized; enforcement of these areas might well not precipitate drastic escalation by the other side.[62] This possibility should be examined further through war gaming, as well as by historical case studies of the use of assertive peacetime Cold War and post–Cold War–era antiscouting tactics, such as shouldering, communications jamming, and physical attack.[63] If the findings are favorable in terms of escalatory risks and the resulting legitimization of the same against American unmanned systems during crises is tolerable, it may be worthwhile for the United States to advance unmanned scout neutralization diplomatically as a norm.

POST–FIRST STRIKE/SALVO OPERATIONS

A defender's most immediate uses of deception and concealment after absorbing a first strike are to prevent, or reduce the effectiveness of, follow-on strikes against forward forces as they reconstitute and then begin their direct resistance. The tactics used are much the same as before the first strike, but their potential effectiveness is amplified by the fact that the defender can now physically neutralize manned scouts and aggressively deceive, if not selectively neutralize, elements of the adversary's maritime surveillance-reconnaissance network.

However, a defender's political objectives will often deny the luxury of waiting for decisive neutralization of the adversary network's capabilities before committing higher-campaign-value forces within the contested zone. Indeed, political direction may compel extremely risky operations, in which forward forces will have to rely heavily on tactical concealment and deception for self-protection.

For example, during the Yom Kippur War the Israeli navy was tasked with removing the Syrian and Egyptian fast-attack-craft threat to coastal commerce, even though the Israelis' Gabriel Mark 1 antiship missile could reach only half as far as their opponents' Soviet-supplied SS-N-2 Styx. Worse, Israeli fast attack craft lacked robust active antiship-missile-defense capabilities. The Israeli navy's main defenses at the time were chaff and shipboard EW jammers whose specifications reportedly owed more to educated guesses than the limited technical intelligence available. Israeli EW systems were therefore designed to employ multiple tricks, in hopes that at least one would prove effective. The design assumptions were vindicated during the Yom Kippur naval battles of Latakia and Baltim, where the Israeli EW lured the Syrian and Egyptian craft into depleting their Styx inventories, which in turn allowed the Israeli craft to close within Gabriel range and devastate their opponents.[64]

A defender may not always be this fortunate in countermeasure-design assumptions and yet be no less pressed to operate deep within an adversary's optimal attack range. The fact that there was little confidence the U.S. Navy's first-generation noise jammers could counter German radio-guided antiship bombs, after all, was not allowed to hold up the September 1943 Salerno landings.[65] This possibility highlights the importance of planning "branching" (alternative) actions, and perhaps also of using, as politically and operationally possible, assets for which losses could be tolerated, to mitigate the impact of failed deception or concealment.

The relaxation of the rules of engagement after a first strike also opens the door to using deception and concealment to distract an adversary from the defender's subsequent actions, mislead the adversary as to the defender's intentions, or seduce him into wasting scarce resources investigating or attacking decoys. This is especially promising if the adversary's decision makers are doctrinally dogmatic; overconfident in their surveillance-reconnaissance-strike capabilities, tactics, and plans; or driven to attack by ideology or fear. Signature-simulating decoy aircraft, vehicles, and equipment can be dispersed to forward land bases, which, when supported by deceptive communications and CNC, may be able to attract attention or attack. Likewise, as demonstrated by the U.S. SCATHE MEAN mission during the 1991 Gulf War, unmanned aerial vehicles or gliding expendable decoys can simulate aircraft in action.[66] Unmanned subsurface vehicles could similarly be used to simulate submarines in order to confuse antisubmarine forces, if not lure them out of position or into wasteful prosecutions.

On the ocean surface, as previously discussed U.S. Navy Cold War–era examples show, it is entirely feasible to surround a ship that is visually and electronically simulating a high-campaign-value unit with actual escorts or aircraft to create a decoy group. A defender may also use signature-emulation technologies

installed in low-campaign-value warships, aircraft, or unmanned systems to form a decoy group.[67] Decoy groups can be positioned in a distant part of a theater to divert attention or attract attack, or they can steam ahead of actual groups to confuse the situational picture, induce the adversary to commit forces prematurely, or lure those forces into an ambush.

Decoy groups are more likely to succeed early in a conflict if the defender has convinced the opponent in peacetime that a certain operational sequence would be followed during hostilities. For instance, although the conditioning effort was not preplanned, decades of operational observations led U.S. Navy commanders, planners, and intelligence analysts to expect the Imperial Japanese Navy to wait in home waters for the U.S. Pacific Fleet's sortie toward East Asia in event of war. By placing decoy units near Japanese homeports to cover the Striking Force's transit, the Imperial Japanese Navy exploited American expectations to great effect.[68] Similarly, if during peacetime exercises a defender has routinely moved a particular unit type or group forward—perhaps even to specific areas—shortly after the "outbreak of hostilities" to perform missions consistent with publicly articulated strategy or doctrine, the attacker might well expect the defender to do the same in an actual conflict. Decoy forces fitting that pattern, supported by efforts to blind or roll back surveillance and reconnaissance coverage, may be very effective—especially if they play directly to the adversary's own preconceptions and doctrinal preferences.

Other forms of deception and concealment that might be used early in a conflict rely on misleading the adversary's decision makers as to operational or tactical intentions and priorities. In a *feint,* deliberate contact with an adversary's forces is made to deceive their commanders as to the timing, location, or importance of the separate, actual main offensive action.[69] For example, during Operation HUSKY, the Allied invasion of Sicily, in July 1943, U.S. Navy "Beach Jumpers" used fast boats armed with barrage rockets and equipped with noisemakers that acoustically simulated landing craft and infantry firefights, smoke-laying gear, and EW systems to conduct feint landing attempts in the western part of the island. These feints resulted in German reserves being withheld from the actual beachhead in southern Sicily. Two months later, the Beach Jumpers seized islands in the Gulf of Naples to confuse the Germans as to the planned landing beach site for Operation AVALANCHE, once again producing German hesitation to commit reserves—this time at Salerno.[70] In contrast, an attempt to entice an opponent, by a "show of force" but without direct contact, into actions favorable to oneself is a *demonstration.*[71] During the first Gulf War, the presence of a U.S. Navy amphibious task force in the northern Arabian Gulf, for instance, served as a demonstration that induced Iraqi misallocation of major forces to guarding Kuwait's coast rather than its land border.[72]

Naval War College Review, Vol. 66 [2013], No. 4, Art. 7

None of these deceptions was in itself of decisive importance to the success of the operations they supported, but all reduced the opposition with which friendly forces had to cope at critical stages. Indeed, well-conceived feints and demonstrations before a main action can induce an adversary to divert surveillance, reconnaissance, or strike resources from positions where they could have been employed against the main force. Afterward, feints and demonstrations may be used to distract attention from follow-on maneuvers as well as to cause confusion as to the friendly force's actual objectives.

Feints and demonstrations generally require the use of actual combatant forces, as opposed to artificial decoys, though the former have historically often been augmented by the latter to achieve desired effects. A deception story might require that certain actions be actually performed rather than simulated, and stand-alone artificial decoys may be unable to keep the adversary deceived for the length of time desired. The visible use of actual forces may also provide a hesitant adversary a "certainty" that will lead to the distraction of attention and misallocation of resources.

Maritime feints and demonstrations might involve actual strikes or localized control/denial operations by submarines or aircraft, threatening movements by naval surface forces, amphibious raids, or simulated amphibious or airborne force insertions, all with the intention of distracting the adversary or drawing combat resources away from a main action. "Cyberfeints" against elements of an adversary's maritime surveillance-reconnaissance-strike network—or perhaps some other network—could even be performed to divert attention and defense resources from cyberspace operations elsewhere, or distract attention from real-world tactical actions.

Feints and demonstrations must not reduce one's own available combat power below what is necessary for high-confidence execution of a main action. Feint and demonstration groups will generally employ concealment, ruses, or displays to attract attention at particular times and places but otherwise to cloak their movements and dispositions. Communications deception and CNC may be used to make the feint or demonstration appear to be the main action. Specially constructed feints and demonstrations may also play to the JOAC's emphasis on seizing the initiative by deploying and operating along multiple, independent lines.[73] Some feints or demonstrations could even conceivably be designed to achieve campaign-level objectives, such as disrupting and wearing down expeditionary or maritime denial forces, reducing confidence in the adversary's surveillance-reconnaissance tactics and network, or seizing peripheral territories useful for forward bases.[74] However, feints and demonstrations using sizable forces or units of medium or high campaign value might not be viable at acceptable risk until

the adversary's surveillance-reconnaissance capabilities are sufficiently degraded or long-range maritime strike arsenals depleted.

Notwithstanding all this, a maritime force must eventually break cover to execute its missions—land-attack strikes, amphibious operations, air and missile defense in support of bases and allied territories, or sea control or denial. Continued deception and concealment for countersurveillance become difficult at this stage. Nonetheless, some forms of countertargeting deception—such as use of decoy units and groups, artificial decoys, or obscurants—might retain effectiveness, depending on the mission and the threat environment.[75] Once the time comes for maritime forces to break contact with the adversary and relocate or withdraw, joint and combined forces' support in the form of feints, demonstrations, or ruses, as well as nonkinetic disruption and physical neutralization of the adversary's surveillance-reconnaissance network assets, would likely prove invaluable.

INTELLIGENCE, TRAINING, ORGANIZATIONAL, AND PLANNING PREREQUISITES

None of the deception and concealment tactics discussed thus far will work absent groundwork begun many years in advance, of which intelligence and counterintelligence preparation is perhaps the most painstaking part. Deception planners must identify the intelligence-collection points of potential adversaries and learn what stimuli are necessary to elicit desired reactions.[76] They also need to understand potential adversaries' surveillance and reconnaissance doctrine and tactics, sensor designs and capabilities, sensor network architecture (including data transmission and fusion), and counterdeception measures. Perhaps most critically, deception planners need to identify maritime operational and tactical leaders of likely opponents and learn as much as possible about their decision-making processes and tendencies.[77]

While some of this information can be collected via clandestine means, much of it depends on repeated, systematically orchestrated operational exposure to the surveillance-reconnaissance networks of potential adversaries. Routine maritime exercises can be tailored to elicit surveillance, reconnaissance, and force-posturing responses. These exercises can also be designed to shape perceptions of friendly forces' doctrine, capabilities, likely wartime campaign priorities, and decision making. Perception shaping is especially important because, as we have seen, the credibility of deception stories in combat increases if an adversary's decision makers have been conditioned in peacetime to anticipate certain behaviors by the defender.

Potential adversaries might restrain their responses to exercises to withhold useful information, or could conceivably tailor responses as deceptions of their

own. Their observed behavior during exercises—as well as their own exercises—can be correlated with other sources to find the probable "ground truth." Military decision makers are often quite frank in their professional journals and military-academic studies about their forces' shortcomings and needed doctrinal, tactical, or technological changes. Open-source writings also provide a window into the thought processes and mentalities of their authors, which is especially useful should those authors be, or eventually become, key decision makers. Counterintelligence on the potential adversary's own collection priorities provides additional data points. Systematic human-in-the-loop war gaming based on what is confidently known about possible opponents' objectives, doctrine, and weapons inventories may also be useful in building or checking potentially actionable assumptions about their "shoot/no-shoot" criteria in prewar and wartime circumstances.[78] Over time, all these sources and methods help in formulating, testing, and evaluating hypotheses regarding adversary capabilities and behaviors relative to various stimuli.

Intelligence and counterintelligence additionally provide feedback regarding the effectiveness of a deception in progress.[79] Since doctrine and operational plans cannot depend on deep and reliable intelligence penetration of the adversary, wartime intelligence feedback may come mostly from the actions of the target of a deception. For instance, a key indicator of success might be that the adversary is focusing surveillance and reconnaissance resources or massing strike assets in ways that appear driven by the deception story. A decrease in adversary data exfiltration efforts from a given network following friendly-force CNC operations might suggest that the adversary is losing confidence in the network's usefulness for intelligence exploitation. Feints and minor operations can also be conducted during a conflict to observe and analyze responses, as a precursor of major initiatives.

Another method for assessing the effectiveness of deception and concealment is the "red team." Intelligence cells not privy to a friendly force's plans can be tasked with deducing that force's location, composition, and intentions using only tools, tactics, and techniques either possessed by or within the capabilities of adversary intelligence. If the red team is able to penetrate the friendly force's deception and concealment, the planned action can be postponed and redesigned or otherwise replaced by a branching action.[80] Indeed, planned branches are particularly critical against contingencies in which the adversary overcomes the friendly force's deception and concealment or successfully employs counterdeception.

Friendly forces must therefore be trained, equipped, and supported to minimize their losses if they must fight their way out should deception or concealment fail. Operational and tactical decision makers must weigh the risk of failure

against the immediate need to accomplish a given mission. If the mission's operational-strategic need is great enough, the risk of major losses if deception and concealment are ineffective might be accepted. If not, the mission might be deferred until the probability of success at tolerable risk, with or without effective deception and concealment, increases.

In any case, deception planning in a theater should be centrally coordinated to ensure that localized deception in support of a given operation or tactical action does not conflict with or compromise others.[81] Deception must be firmly integrated within and subordinated to the force-level commander's overall plan of action. Commanders must ensure that all units or groups under their control understand their roles in a deception so that inadvertent or independent actions do not gradually undermine it. This is difficult enough to accomplish within a single-service organization, such as a carrier group; the addition of other services or allied forces compounds the challenge. Regular peacetime exercises are the best venues for working out these issues; it may not be possible to do so effectively in the heat of crisis. The deception plan itself must be flexible enough that necessary measures or inadvertent incidents that break the cover can be made to appear consistent with the story. Above all, the story must be plausible with respect to the existing situation, consistent with the prior shaping of expectations and perceptions, and tailored to exploit the opponent's apparent processes and inclinations.[82]

Deception and concealment concepts must be aggressively tested in the context of force-level doctrine and tactics. For instance, subtle differences in decoy positioning relative to main forces and defended units might mean failure.[83] Modeling and simulation, with and without humans in the loop, should be used for preliminary concept testing. Thereafter, however, battle experiments conducted during training exercises are critical for validation.[84]

It follows that forces must be thoroughly trained for performing deception and concealment while executing operations and tactical actions. Deception and concealment plans may require consumption of fuel and stores at a higher rate than would otherwise be the case, and the logistical challenges that may arise must be appreciated. In addition, friendly forces must be capable of executing deception and concealment safely despite the constraints they place on communications and active sensors. Personnel safety, not to mention that of ships and aircraft, depends on crew familiarity with operating in restrictive EMCON and intense cyber-electronic-warfare environments.[85] Increasing unit-level initiative in keeping with a commander's promulgated intentions will be a particularly critical training objective. This emphasis may require the focused advocacy of senior leadership, given the ways it runs contrary to certain network-centric warfare practices of the past two decades.[86]

Naval War College Review, Vol. 66 [2013], No. 4, Art. 7

Some doctrinal elements or tactics that are considered war-critical, as well as tactical situations too complex to generate in forward theaters, can be practiced in home operating areas. In-port synthetic training can also be used for these purposes; it has the added benefits of enabling more frequent and intensive training than may be possible at sea, given how budgetary constraints are increasingly curtailing exercises of nondeployed forces. That said, aggressive peacetime training at sea remains necessary to provide the environmental variability and operational risks necessary for building proficiency in deception and concealment. High-confidence intelligence, advanced technologies, and a clever deception plan may be all for naught if a force's personnel lack the conditioning to execute the plan safely and reliably.

"Training like you'd fight" and efforts to condition a potential adversary's perceptions during peacetime are not necessarily incompatible. An exercise's primary purpose is to increase proficiency in executing doctrine and tactics. As noted earlier, however, this does not mean that exercise scenarios must closely mirror actual campaign plans. It bears repeating that if forward exercises and authoritative public expressions of strategy and doctrine create an impression that the United States and its allies would follow a certain operational sequence in a given contingency, a potential adversary might be conditioned to believe that it reflects the actual contingency plan. None of this would degrade the ability of exercise forces to train to their doctrinal and tactical objectives.

CONCEALMENT, DECEPTION, AND DETERRENCE

Exercises designed to shape perceptions can serve an additional purpose—reinforcing deterrence. If risk-averse prospective aggressors can be convinced by peacetime demonstrations of selected deception and concealment capabilities that their chances of detecting and identifying forces are low or extremely uncertain, and their opportunity costs of wasting advanced weapons are high, they may estimate that their prospects for a decisive first strike are insufficiently promising. Even if these prospective aggressors believe an opening attack might land strategically exploitable tactical blows, they may still be deterred if brought to conclude that the surviving defenders, now freed of prior restrictions on physical and cyber-electronic responses, would retain a fair chance of preventing the offensive from achieving its political objectives.

There is precedent in modern American military history for maritime demonstrations along these lines. As we have seen, the U.S. Navy selectively demonstrated deception and concealment capabilities throughout the Cold War as a means of lessening the confidence of Soviet leaders in the SOSS while simultaneously eliciting observable political and military reactions. During the first half of the 1980s in particular, the Navy wove these demonstrations into exercises

along the periphery of the Soviet Union as part of a joint psychological campaign supporting specific grand-strategic objectives, along with military intelligence collection.[87] These exercises were also likely designed to "normalize" U.S. use of deception and concealment, as to reduce the risk that their employment during heightened tensions might be misperceived as signaling hostile intent, as well as to shape Soviet expectations regarding U.S. maritime doctrine, campaign priorities, and strategy for a NATO–Warsaw Pact conflict. The exercises were certainly successful from the American perspective in terms of the intelligence collected, and eventual declassification of archival materials will reveal how they were viewed by both sides in terms of deterrence and conditioning.[88]

A deterrence-reinforcing psychological campaign of that scope and scale is neither necessary nor desirable against China today, though an appropriately scaled campaign aimed at deterring Iranian conventional aggression might be, as the impasse over Tehran's nuclear program continues to fester. Nevertheless, routine exercises in the western Pacific, conducted within view of China's nascent ocean-surveillance system, should periodically include psychological conditioning elements configured to shape expectations, as well as concealment and deception tactics selected to buttress the conventional deterrence credibility of U.S. maritime forces. Visible commitment to training the joint force in the practice of maritime concealment and deception, selectively publicized acquisition of related technologies, and judicious demonstration of those tactics and technologies may, in coordination with grand-strategic initiatives featuring other elements of U.S. and allied power, go a long way toward enhancing conventional deterrence. Should deterrence fail, though, these same measures would likely prove invaluable in having shaped an operational theater during peacetime in a way that promoted access in war—perhaps the most important precept of the *Joint Operational Access Concept.*[89]

NOTES

1. U.S. Joint Staff, *Joint Operational Access Concept, Version 1.0* (Washington, D.C.: 17 January 2012) [hereafter *Joint Operational Access Concept*], pp. 3–4. As a terminology note, this article defines "maritime control" and "maritime denial" by expanding on Julian Corbett's definitions of "sea control" and "sea denial." Corbett asserts that navies can never control the entirety of a sea at all times. Instead, he argues, navies strive to obtain and exercise temporary control of localized sea areas for given purposes or otherwise strive to prevent opponents from obtaining and exercising temporary localized sea control. The same is arguably true about military activities in the air and on land. Since a force can use any one of these domains to support localized control in any of the other domains and can likewise use any of these domains to prevent or contest an adversary's localized control in any of the other domains, new Corbettian terminology is needed that accounts for these interactions. Given that a maritime area combines the sea with the airspace and "landspace" that

Naval War College Review, Vol. 66 [2013], No. 4, Art. 7

can affect or be affected by an actor's use of the sea, "maritime control" means that a force (whether single-service, joint, or combined) has obtained and is exercising control of a localized maritime area for a certain duration and purpose; "maritime denial" means that a force is challenging an opposing force's efforts to obtain and exercise control of a localized maritime area.

2. Ibid., pp. 2, 22–23, 25–26, 30–31.

3. The term "force level" describes the doctrine, tactics, capabilities, operating concepts, and other considerations applicable to operating a maritime single-service, joint, or combined task force or group as an integrated whole.

4. Wide-area surveillance sensors and mobile, highly sensitive reconnaissance sensors are arguably the most lucrative targets in an anti-network campaign, as they cannot be repaired or replaced quickly or cheaply. Conversely, it is neither expensive nor time consuming in relative terms to replace damaged network computing infrastructure or shift to backup command sites. The only tactically meaningful cost imposed by physical attacks against computing infrastructure may be the adversary network's temporary (albeit graceful, if the network is well designed) degradation, which friendly forces can certainly exploit operationally or tactically while it lasts.

5. For examples of these tasks in the context of notional conflicts with China or Iran, see Mark Gunzinger, with Chris Dougherty, *Outside-In: Operating from Range to Defeat Iran's Anti-access and Area-Denial Threats* (Washington, D.C.: Center for Strategic and Budgetary Assessments, January 2012), pp. 53–73; Jan Van Tol [Capt., USN (Ret.)] et al., *AirSea Battle: A Point of Departure Operational Concept* (Washington, D.C.: Center for Strategic and Budgetary Assessments, May 2010), pp. 56, 60, 74, 76, 117; and Jonathan F. Solomon, "Defending the Fleet from China's Anti-ship Ballistic Missile: Naval Deception's Roles in Sea-Based Missile Defense" (master's thesis, Georgetown University, 2011), pp. 114–15, 130–31, available at http://repository.library.georgetown.edu/.

6. Although it is unclear whether the Iraqi Kari integrated air-defense system had been designed with war-reserve capabilities including redundant communications pathways, it was able to retain limited yet effective combat functionality in certain areas of Iraq despite debilitating strikes against its command-and-control nodes. The United States was never able to sever Kari's communications pathways fully, and the Iraqis were apparently even able to "regenerate" some nodes in spite of the punishment they absorbed. See Michael R. Gordon and Bernard E. Trainor [Lt. Gen., USMC (Ret.)], *The General's War* (Boston: Back Bay Books, 1995), pp. 256–57.

7. U.S. Joint Staff, *Military Deception,* Joint Publication 3-13.4 (Washington D.C.: 26 January 2012) [hereafter JP 3-13.4], pp. II-8–II-9.

8. *Joint Operational Access Concept,* p. 25.

9. For example, inadequately positioned active-sensing platforms decisively undermined a naval battle force's EMCON during 1957 U.S. Navy fleet experimentation with concealment and deception. See Robert G. Angevine, "Hiding in Plain Sight: The U.S. Navy and Dispersed Operations under EMCON, 1956–1972," *Naval War College Review* 64, no. 2 (Spring 2011), p. 82.

10. Norman Friedman, *Network-centric Warfare: How Navies Learned to Fight Smarter through Three World Wars* (Annapolis, Md.: Naval Institute Press, 2009), pp. 233–35, 237–38.

11. Angevine, "Hiding in Plain Sight," pp. 89–92.

12. An example of this is the U.S. Navy's Cold War–era exploitation of the poor sensitivity of Soviet radar ocean-reconnaissance satellites (RORSATs). RORSATs were continuously tracked and reported to U.S. naval forces so that large warships, such as aircraft carriers, could maneuver to present their smallest radar cross sections as satellites passed overhead; see Norman Friedman, *Seapower and Space: From the Dawn of the Missile Age to Net-centric Warfare* (Annapolis, Md.: Naval Institute Press, 2000), p. 195. Similarly, stricter EMCON periods were scheduled for when Soviet ELINT ocean-reconnaissance satellites were expected to be overhead; see Friedman, *Network-centric Warfare,* pp. 237–38.

13. For example, a combined U.S. and NATO battle force transiting from Norfolk, Virginia, to the Norwegian Sea for exercises Ocean Safari and Magic Sword North in August –September 1981 reportedly used a passing North Atlantic hurricane for cover from

Soviet surveillance and reconnaissance; see Gregory L. Vistica, *Fall from Glory: The Men Who Sank the U.S. Navy* (New York: Touchstone, 1997), pp. 117–18. Vistica's interesting descriptions of other U.S. Navy deception and concealment tactics employed against the SOSS during this exercise should be viewed differently from the rest of his book; see Solomon, "Defending the Fleet from China's Anti-ship Ballistic Missile," p. 61.

14. An example of how the U.S. Navy has exploited this kind of vulnerability in the past involves RORSAT's poor clutter-rejection capabilities. See Friedman, *Seapower and Space,* p. 195.

15. For more on obscurants for countertargeting, see Thomas J. Culora, "The Strategic Implications of Obscurants: History and the Future," *Naval War College Review* 63, no. 3 (Summer 2010), pp. 73–84, and Scott Tait [Cdr., USN], "Make Smoke!," U.S. Naval Institute *Proceedings* 137, no. 6 (June 2011), pp. 58–63.

16. The traditional term "high-value unit" is shorthand for tactically important or very expensive assets that a force must strive to protect: aircraft carriers, amphibious and maritime prepositioned matériel–carrying ships, replenishment ships, strategic aircraft, wide-area-surveillance aircraft, transport aircraft, and airborne-refueling aircraft. At the spectrum's other end, "low-value unit" applies to relatively expendable small surface combatants and tactical aircraft. This terminology is imprecise, however, in that it incorrectly implies that an asset's *tactical* value always carries over into *campaign-level* value. Although "high-value units" generally have high campaign value, the relationship is not automatic. For example, while an aircraft carrier's tactical value is difficult to dispute, in a given campaign a combatant capable of ballistic-missile defense or a submarine carrying conventional land-attack missiles—either of which might otherwise be considered medium-value units—may be of greater importance and correspondingly require the support of the rest of the force. The key to interpreting a specific asset's campaign value is to judge how a campaign would be impacted by its temporary incapacitation or outright loss. Campaign value is thus a more nuanced framework for doctrinal development and operational planning.

17. For examples of U.S. Navy dispersed formation tactics during the Cold War, see Angevine, "Hiding in Plain Sight," pp. 80–88, and Friedman, *Network-centric Warfare,* p. 238.

18. Adm. Isoroku Yamamoto's operational plan for Midway is a case study in how not to structure maritime dispersal for deception and concealment. By threatening to seize Midway, Yamamoto sought to lure the U.S. Pacific Fleet's carriers into decisive battle. However, rather than intentionally use his 1st Air Fleet carriers as his primary spear, the lethal blow was to come from his battleships, in a night action. His concept of operations therefore positioned the battleship main body, for its own concealment, hundreds of miles from the 1st Air Fleet. That made it impossible to add battleships to the 1st Air Fleet's air defenses in the event his assumption of operational surprise proved incorrect. Yamamoto also inexplicably chose not to augment the 1st Air Fleet's screening and scouting resources with the fast destroyers and floatplane-equipped cruisers meant eventually to provide fire support to the Midway landing force. By rendering the majority of his fleet incapable of supporting his highest-campaign-value warships, Yamamoto ensured that the resulting exchange would be isolated to the opposing and fairly closely matched carrier forces. See Jonathan Parshall and Anthony Tully, *Shattered Sword: The Untold Story of the Battle of Midway* (Washington, D.C.: Potomac Books, 2005), pp. 50, 53–56.

19. Milan N. Vego, "Operational Deception in the Information Age," *Joint Force Quarterly,* no. 30 (Spring 2002), pp. 60–66. As an example, the Imperial Japanese Navy's Pearl Harbor Striking Force employed strict OPSEC and COMSEC measures to conceal its November–December 1941 transit to the Hawaiian Islands for the Pearl Harbor raid. See Gordon W. Prange, *At Dawn We Slept: The Untold Story of Pearl Harbor* (New York: McGraw-Hill, 1981), pp. 376–77, 379, 420, and Robert J. Hanyok, "'Catching the Fox Unaware': Japanese Radio Denial and Deception and the Attack on Pearl Harbor," *Naval War College Review* 61, no. 4 (Autumn 2008), pp. 103, 106–10, 114.

20. The U.S. Navy experimented during the Cold War era with human couriers to enhance

OPSEC and COMSEC. See Angevine, "Hiding in Plain Sight," p. 89, and Vistica, *Fall from Glory,* p. 108.

21. For an outstanding technical overview of RF LPI, including theoretical LPI countermeasure technologies and techniques, see Aytug Denk [Capt., Turkish air force], "Detection and Jamming Low Probability of Intercept (LPI) Radars" (master's thesis, U.S. Naval Postgraduate School, September 2006). It seems doubtful that LPI systems can avoid resort to restrictive EMCON within a contested area for the duration of a conflict. While a highly directional line-of-sight RF communications system might employ LPI capabilities actively with acceptable risk, as that beam is very difficult to intercept, the same would not be true of a search radar. LPI seems to hold more promise as a means for expanding transmissions under certain risk-defined circumstances during EMCON than as a complete substitute for EMCON.

22. RF noise jamming is an especially attractive option for cutting off an adversary's scouts and space-based surveillance sensors from networks, decreasing the timeliness and throughput of their communications, or forcing them to maneuver evasively in ways that benefit a defended force. In fact, co-orbital minisatellite jammers represent a potential option for nonkinetically attacking data-relay satellites, which are critical nodes in wide-area maritime surveillance-reconnaissance networks. Communications jamming against a potential adversary's satellites might be unduly escalatory in a crisis, so its use would almost certainly be a political decision; should hostilities erupt, though, it would be far less escalatory and damaging to the orbital environment than a kinetic kill. See Stephen Latchford [Lt. Col., USAF], *Strategies for Defeating Commercial Imagery Systems,* Occasional Paper 39 (Maxwell Air Force Base [hereafter AFB], Ala.: Center for Strategy and Technology, Air Univ., December 2005), pp. 22–23.

23. Ibid., p. 24.

24. JP 3-13.4, pp. I-1, I-4.

25. For example, although Allied bombers neutralized most major surveillance-radar sites in southern France prior to the August 1944 DRAGOON landings, one major site was spared to support a deception involving simulation of an assault force approaching a different area. See Thaddeus Holt, *The Deceivers: Allied Military Deception in the Second World War* (New York: Skyhorse, 2007), p. 619.

26. See Michael Howard, *British Intelligence in the Second World War,* vol. 5, *Strategic Deception* (Cambridge, U.K.: Cambridge Univ. Press, 1990), p. 224, and Holt, *Deceivers,* pp. 83–84. Holt also notes that in World War II the U.S. Navy developed tactics for disguising low-campaign-value warships as units of higher value but does not seem to have employed them widely.

27. Examples include the use by the Algiers landing force during Operation TORCH in November 1942 of a route that implied until the last moment it was a Malta supply convoy, and by the DRAGOON landing force of a track that reinforced German expectations that the Genoa region would be the next Allied objective. See Francis Harry Hinsley, *British Intelligence in the Second World War,* abridged version (Cambridge, U.K.: Cambridge Univ. Press, 1993), p. 259, and Holt, *Deceivers,* p. 619.

28. See Friedman, *Network-centric Warfare,* pp. 233–35.

29. For example, this tactic was used by kamikaze raiders during World War II, as well as by the Iraqi air force in a nearly successful strike against critical Saudi oil infrastructure during the first Gulf War. See John Monsarrat, *Angel on the Yardarm: The Beginnings of Fleet Radar Defense and the Kamikaze Threat* (Newport, R.I.: Naval War College Press, 1985), pp. 130–34; Robert Stern, *Fire from the Sky: Surviving the Kamikaze Threat* (Annapolis, Md.: Naval Institute Press, 2010), p. 321; and Gordon and Trainor, *General's War,* pp. 263–66.

30. Anti–pattern analysis tactics can include deceptively positioned transmitting stations and simulation of transmitter or operator signature characteristics to misrepresent a unit's identity or mission. Other tactics include manipulating the volume, priority, or classification of message traffic to generate false "peaks" and "troughs" so as to conceal the actual pattern. "Offensive manipulation" uses these tactics to mislead the adversary as to the units, locations, activities, and timing associated with an operation or action. "Defensive manipulation" increases the traffic

on channels typically associated with forces or locations not involved in a planned event while suppressing activity associated with units, etc., that are. In preparation for anti–pattern analysis measures, deception teams collect traffic-pattern data of a unit or force, as well as representative samples of message content over a long period, including both routine (in port or in garrison) and elevated (preparation for, or execution of, missions) levels of activity. The unit's or force's communications can then be modeled and simulated with appropriate fidelity; for these tactics as applied during World War II, see Holt, *Deceivers,* pp. 85–92. Though originally conceived for use against data and voice radio, anti–pattern analysis tactics are also extensible to cyberdeception.

31. Military communications facilities in Japan supported the Striking Force with daily information broadcasts on the same schedule and frequencies used during late-1941 exercises in home waters. Intricate deceptive transmissions were also made from Japanese home ports to simulate Striking Force units. These measures, combined with the actual force's high-frequency radio EMCON, had the effect of convincing U.S. radio-traffic analysts that the force was still near Japan. Their analysis was further degraded by Japanese units' use of multiple call signs—or none at all—to defeat correlation. Lastly, observable Japanese communications patterns immediately prior to Pearl Harbor were significantly different from those seen during previous periods of intensive activity, denying U.S. intelligence a key indicator. See Prange, *At Dawn We Slept,* pp. 338, 353–54, 362, 424–25, 427, 440–42, and Hanyok, "'Catching the Fox Unaware,'" pp. 104–12.

32. John B. Dwyer, *Seaborne Deception: The History of U.S. Navy Beach Jumpers* (New York: Praeger, 1992), pp. 102, 127–28.

33. Imitative deception is very difficult, as it requires at a minimum detailed knowledge of the adversary's communications procedures, authentication measures, and equipment and operator characteristics. It is generally not a primary deception tactic. See Holt, *Deceivers,* p. 93.

34. See ibid., pp. 89, 578, 619; Dwyer, *Seaborne Deception,* pp. 25–33, 35–48, 79; and Monsarrat, *Angel on the Yardarm,* pp. 126–27.

35. For IFF spoofing by Japanese kamikazes, see Stern, *Fire from the Sky,* p. 155. For a thorough technical overview of the EW waged between developers of German radio-guided antiship bombs and Allied defensive countermeasures, see Martin J. Bollinger, *Warriors and Wizards: The Development and Defeat of Radio-Controlled Glide Bombs of the Third Reich* (Annapolis, Md.: Naval Institute Press, 2010).

36. For the U.S. Navy's 1960s-era AN/ULQ-5 and -6 blip enhancers, see Dwyer, *Seaborne Deception,* p. 102. For the 1970s- and- '80s-era AN/SSQ-74 Integrated Cover and Deception System (ICADS), see Friedman, *Network-centric Warfare,* pp. 247, 343. Per Friedman, ICADS was housed in a trailer temporarily installed on a warship's flight deck. ICADS Phase 1 allowed its host to simulate an aircraft carrier's telltale radios and radars. ICADS Phase 2 added a false-target generator that could deceive Soviet airborne and RORSAT radars, as well as an acoustic element that simulated a carrier's machinery noise to deceive Soviet submarines. For an overview of mid-to-late-twentieth-century deceptive EW techniques and expendable offboard decoy technologies, see Solomon, "Defending the Fleet from China's Anti-ship Ballistic Missile," pp. 81–87.

37. See Kenneth Helberg et al., *Electronic Warfare Technology Trends and Visions* (Wright-Patterson AFB, Ohio: Research Development Center, May 1990), pp. 5–7, and P. E. Pace et al., *Digital Image Synthesizers: Are Enemy Sensors Really Seeing What's There?* (Monterey, Calif.: Naval Postgraduate School, 15 November 2004).

38. "Computer network charade," or CNC, is a term suggested by an anonymous reviewer of this article, to whom I am grateful for the idea.

39. For outstanding summaries of the potential uses of disinformation planting and honeypots for CNC, as well as the theoretical impact of CNC on an adversary's intelligence collection efforts, see Fred Cohen, "The Use of Deception Techniques: Honeypots and Decoys," n.d., available at all.net/journal/deception/Deception_Techniques_.pdf, and Neil C. Rowe, *Deception in Defense of Computer Systems from Cyber-Attack* (Monterey, Calif.: Naval Postgraduate School, n.d.), available at faculty.nps.edu/. Rowe's paper

also summarizes high-fidelity deceptive simulation of an actual node's or network's behavior. As with preparation for communications deception, if a CNC deception team has access to node or network behavioral data and representative content over the range of operating tempos, it ought to be able to model and then simulate them in another node/network or in a honeypot or net. This is an important area for unit- and force-level experimentation.

40. This hypothetical CNC tactic is envisioned for the Nonsecure Internet Protocol Router Network (NIPRNet) and perhaps also the Secure Internet Protocol Router Network (SIPRNet). It is not envisioned for operational or tactical data-link or distributed fire-control networks.

41. CNC's relative immaturity means that its viability must be proved in war games, battle experiments, and developmental tests before it can be incorporated in doctrine and operational plans. CNC may well prove more useful for concealment (saturating adversary collection systems and overwhelming decision makers with sheer volume and ambiguity) than for outright deception. A potentially useful way to estimate its combat efficacy would be to study historical cases of equivalent communications deception. For example, in spring 1942, U.S. naval intelligence used a false, unencrypted radio message about Midway Island's water-purification system to elicit enemy communications activity that helped verify that Midway was indeed the Imperial Japanese Navy's next target; see Patrick D. Weadon, "The Battle of Midway," *National Security Agency / Central Security Service,* 15 January 2009, www.nsa.gov/. There is little conceptual difference between this episode and how CNC might be used in the future.

42. The challenges of rapidly obtaining and reacting to I&W may make it extremely difficult to use decoy forces to successfully induce an adversary into wasting precious first-strike resources. It also brings the danger of premature employment of "crown jewel" deception tactics. Nevertheless, defending leaders who are confident that they understand their counterparts' mind-sets and perceptions well enough, have sufficient maneuver space, and judge the probability of war to be high may decide that even a failed decoy attempt is better than waiting passively for their counterparts' first move.

43. As an example, a Royal Navy sloop that was attacked during the Luftwaffe's 27 August 1943 radio-guided antiship bombing raid—the second successful one of the war—had on board a Royal Air Force ELINT collection team. This embarkation was not typical, which suggests British intelligence had anticipated the combat debut of the weapon and sought to use a relatively low-campaign-value task group to collect data that would be useful for defending more important forces later. In fact, there is circumstantial evidence the sloop's group was deliberately exposed to attract radio-guided antiship bomb attacks; see Bollinger, *Warriors and Wizards,* pp. 6–8, 49. A sensor's emissions or a weapon's kinematics may very well give away design vulnerabilities that, not easily or rapidly correctable, can be readily exploited by countermeasures. The same may be true of surveillance-reconnaissance-strike tactics and decision making, in which case early data collection may be as important to the defender as inducing the adversary to waste weapons.

44. This point is exemplified by the April–July 1945 Okinawa kamikaze campaign. The raids were initially high in strength and frequency but gradually—though they remained lethal—decreased to relative nuisance levels as it became apparent to Japanese commanders that they were not inflicting significant operational or strategic handicaps on the U.S. Navy and that new production could barely compensate for the aircraft expended. The Japanese decided to husband their remaining inventory for intense raids against U.S. forces during the anticipated invasion of the home islands; see Robin L. Rielly, *Kamikazes, Corsairs, and Picket Ships: Okinawa 1945* (Havertown, Pa.: Casemate, 2008), pp. 312–13, 320–22.

    Luftwaffe patterns in employing radio-guided antiship bombs between July 1943 and August 1944 also represent an example. Severe attrition of the specially configured bombers and corresponding losses of highly trained crews in exchange for no operational gain led to the redeployment of several bomber units from the Mediterranean to

northern Germany for a planned (though never executed) future offensive. Mediterranean radio-guided bombing operations were heavily reduced until the Anzio landings in late January 1944, where heavy attrition led to the withdrawal of most of the surviving bombers in anticipation of the Allied invasion of France. By that time, though, sustained radio-guided bombing operations were all but impossible owing to inadequate bomber and bomb production. See Bollinger, *Warriors and Wizards,* pp. 73–74, 88, 118, 145–49.

45. For experimentally obtained evidence regarding the lingering psychological effects of a successful deception on an adversary's decision making and tactics, albeit in the cyber realm, see Cohen, "Use of Deception Techniques," pp. 17, 19–20.

46. See Solomon, "Defending the Fleet from China's Anti-ship Ballistic Missile," pp. 40–41, 45–49, 54–57.

47. This is the exact principle around which U.S. Navy deception and concealment against the SOSS was structured throughout the Cold War. See Friedman, *Network-centric Warfare,* p. 224.

48. Though adversaries often use deception and concealment to cover first-strike/salvo forces as they increase combat readiness and move into position, they may also employ deception within the first strikes/salvos themselves. The attacker could launch an initial salvo of obsolescent weapons or decoys to entice a defending force into revealing its location or expending ordnance (or revealing defensive EW "tricks"), thereby paving the way for the actual strike. Defenders might be able to defeat such deception by positioning networked multi-phenomenology sensors in their outer defense-in-depth layers to enable early classification of inbound threats, with sensor data relayed by highly directional line-of-sight pathways to mitigate interception risk. Better still is to have a very deep defensive-ordnance inventory that can support many engagements before reloading is needed. This may not be practical with respect to missile interceptors, which suggests the importance of EW countermeasures and future directed-energy defenses. The ideal option, though, is a counterdeception that lures the attacker into wasting salvos. This would be very difficult to orchestrate in peacetime's waning moments but would seem to offer the greatest reward at the least relative cost.

    The attacker can, alternatively, use sacrificial scouts or raiders to elicit defensive responses and thereby reveal a force's positions. This gambit could be countered by positioning the outer defensive layers far enough from the main force so that the former's actions do not directly reveal the latter's location. Following the first strike/salvo, offensive counterair sweeps well forward of a main force can also be used to locate and neutralize adversary scouts. The U.S. Navy's "Outer Air Battle" doctrine and tactics of the late Cold War are examples of these approaches. See Friedman, *Seapower and Space,* pp. 234–39.

49. Richard K. Betts, *Surprise Attack* (Washington, D.C.: Brookings Institution, 1982), pp. 87–141, 155–56. The psychological factors may be especially decisive. A 1975 U.S. Navy war game suggested that a Soviet first salvo's effectiveness might owe more to the targeted crews' shock upon realizing that inbound weapons were real and a war had begun than to their ships' defensive limitations. See Friedman, *Seapower and Space,* p. 346.

50. Lyle J. Goldstein and Yuri M. Zhukov, "A Tale of Two Fleets: A Russian Perspective on the 1973 Naval Standoff in the Mediterranean," *Naval War College Review* 57, no. 2 (Spring 2004), pp. 27–63.

51. Abraham Rabinovich, *The Yom Kippur War: The Epic Encounter That Transformed the Middle East* (New York: Schocken Books, 2004), pp. 478–79, 483–85.

52. Tait, "Make Smoke!," pp. 60–61.

53. Optimal first-strike range is not necessarily the same as the maximum physical reach of the longest-ranged weapon system effective against a given target type (i.e., the combined range of the firing platform and the weapon it carries). Rather, it is defined by trade-offs in surveillance and reconnaissance effectiveness and in the number of weapons employable in a short time as the target's distance from the firing platform's starting position increases. This means that a potential adversary with a weapon system that can reach distance *D* from the homeland's border but can achieve timely and high-confidence peacetime cueing

Naval War College Review, Vol. 66 [2013], No. 4, Art. 7

or targeting only within a radius of 0.75*D* has an optimal first-strike range of 0.75*D*. It follows that if, for technical, operational, or logistical reasons, the adversary can fire only a few *D*-range weapons within a defined short period of time, and if his doctrine therefore calls for using *D*-range weapons in coordination with far more plentiful weapons of range 0.5*D,* the optimal first-strike range decreases to 0.5*D*. This does not reduce the dangers faced by the defender at distance *D* but does offer more flexibility in using force-level doctrine, posture, plans, and capabilities to manage risks.

54. See Solomon, "Defending the Fleet from China's Anti-ship Ballistic Missile," p. 131.

55. These frontline forces have great capacity to blunt an adversary's offensive, and many are either relatively invulnerable to countermeasures (e.g., submarines, mines) or expendable from the campaign-level standpoint (e.g., small warships, land-based antiship missiles). The types, numbers, capabilities, and positions of these frontline units are driven by the threat as well as geography. Defense in a choke point, archipelago, or small physically enclosed sea can be very different from defense in a large marginal sea. Environmental and endurance factors in the former might weight the structure of low-campaign-value forces toward missile-armed patrol boats and short-range, rotary- or fixed-wing aircraft, while those factors in the latter might favor corvette or frigate-type warships and medium-range, fixed-wing aircraft. Additionally, ground-force preinsertion assumes that a remote, isolated territory is strategically worth holding. Depending on geography, operational needs, and the adversary's combat and logistics capabilities, it may be strategically beneficial, in both political and military terms, to induce the adversary's seizure of a given friendly territory. The defender can then wage maritime-denial operations that gradually shift the overall theater correlation of forces in his favor—an important element not only for eventually retaking the territory but also for follow-on operations, maintaining popular support for the war effort, and the eventual political settlement. All this may not be possible, though, if the territory must be held as a barrier against the adversary's open-ocean access.

56. The high-campaign-value-unit positioning argument is convincingly made in Robert C. Rubel, "Talking about Sea Control," *Naval War College Review* 63, no. 4 (Autumn 2010), pp. 38–47. Aspects of the aircraft-carrier-doctrinal-roles argument are advanced in the same author's "The Future of Aircraft Carriers," *Naval War College Review* 64, no. 4 (Autumn 2011), pp. 13–27. Rubel asserts that a carrier's chief future roles in intensely contested oceanic waters should be (using its air wing) maritime surveillance and reconnaissance, support of wide-area communications, and undersea warfare. Rubel downplays the carrier's role in other maritime-control/denial operations, in light of potential adversaries' rapidly improving long-range antiship and air-defense capabilities. However, much as the (modular) air wing represents the carrier's combat power, (modular) ordnance in turn represents the air wing's combat power. In other words, the air wing allows a task group to launch ordnance farther from the main body than if weapons are directly launched by its ships (or submarines); also, the air wing can be quickly reloaded aboard the carrier for follow-on missions, whereas shipboard and submarine launch tubes presently cannot be reloaded at sea. This means that not only does an air wing equipped with standoff antiship and ground-attack ordnance provide a naval force with its most rapidly reloadable spears but that in a prolonged maritime battle consisting of numerous sequential engagements, the same air wing, equipped with standoff antiair and antisubmarine ordnance, provides maritime forces with their most agile and longest-reaching shield.

57. See Solomon, "Defending the Fleet from China's Anti-ship Ballistic Missile," pp. 114–15.

58. Ruses are defined as actions intended to deliberately expose false or ambiguous information to the adversary. They do not necessarily require use of actual combatant forces. See JP 3-13.4, p. I-9.

59. Data collected during a first salvo against them, though, might prove invaluable for deception and concealment during subsequent operations and tactical actions.

60. A "display" is defined as the static "simulation, disguising, or portrayal of friendly objects, units, or capabilities" meant to support

a deception story. It does not necessarily require actual combatant forces. JP3-13.4, pp. I-9, GL-4.

61. For examples, "Russia 'Shot Down Georgia Drone,'" *BBC News,* 21 April 2008, news.bbc.co.uk/; "Iran Fired at Unarmed US Drone, Pentagon Says," *Fox News,* 8 November 2012, www.foxnews.com/.

62. A potential adversary could overcome this threat by placing unmanned systems under close manned escort, but that would undercut the rationale for using unmanned, vice manned, reconnaissance systems to increase search volume and on-station time per sortie. Also, it is not clear how a potential adversary could respond without disproportionate escalation if a defender neutralized the unmanned system by close-in jamming or other nonkinetic means. The point is worth study through war gaming.

63. Interestingly, during an early 1970s U.S. Navy war game it was suggested that since Soviet first-salvo doctrine relied heavily on scouting, the president could warn his Soviet counterpart over the hotline that the approach of any Soviet aircraft within fifty nautical miles of a U.S. aircraft carrier would be interpreted as an act of war. This was deemed unrealistic by the game's participants, though, as it would place on the United States responsibility for the "last clear chance" to avoid a shooting war; see Friedman, *Seapower and Space,* p. 174. With unmanned systems taking on this reconnaissance role, though, it seems less clear that the same escalatory risk now arises.

64. Abraham Rabinovich, *The Boats of Cherbourg: The Secret Israeli Operation That Revolutionized Naval Warfare* (Annapolis, Md.: Naval Institute Press, 1988), pp. 85, 211–53, 258–62.

65. Bollinger, *Warriors and Wizards,* pp. 55–57, 59, 66–67.

66. In SCATHE MEAN, on the opening night of the first Gulf War, 17 January 1991, a U.S. Air Force unit launched BQM-74 target drones and Navy A-6 bombers released tactical air-launched decoys in support of second-wave F-117 strikes against Baghdad. The SCATHE MEAN decoys enticed Iraqi air-defense sites to switch on their targeting radars, which were then subjected to withering antiradiation-missile attacks. The decoys also lured the Iraqis into wasting surface-to-air missiles against false targets. Lastly, the decoys distracted the Iraqis from any intermittent contact their very-high-frequency search radars may have gained against the F-117s. Gordon and Trainor, *General's War,* pp. 112–14, 217, 219–20.

67. For examples, see Solomon, "Defending the Fleet from China's Anti-ship Ballistic Missile," pp. 115–18.

68. Hanyok, "'Catching the Fox Unaware,'" pp. 101–102, 118–19.

69. JP 3-13.4, p. I-9.

70. Dwyer, *Seaborne Deception,* pp. 25–33, 35–48. The British conducted similar maritime feints in support of the June 1944 OVERLORD landings. See Holt, *Deceivers,* p. 578.

71. JP 3-13.4, pp. I-9, GL-4.

72. The U.S. Navy and Marine Corps originally planned an actual, major amphibious assault on the Kuwaiti coast as part of the ground offensive in Operation DESERT STORM. When U.S. Central Command refused to authorize the assault, the amphibious force's presence became a demonstration "by default." See Gordon and Trainor, *General's War,* pp. 293–94.

73. *Joint Operational Access Concept,* pp. 20–21.

74. As an example, Allied bombing missions against western France immediately prior to the OVERLORD landings hit many targets north of the Seine River to lend credence to the FORTITUDE SOUTH story that the primary invasion target was the Pas de Calais. These feint raids, though, secondarily supported OVERLORD by disrupting German movements across the Seine. See Holt, *Deceivers,* p. 94.

75. *Joint Operational Access Concept,* p. 31.

76. For example, early in World War II the Royal Navy attempted to lure Luftwaffe raiders into attacking decoy ships at Rosyth instead of the main fleet at Scapa Flow. The deception ultimately failed; Luftwaffe scouts may never have come across the decoys, and in any case British intelligence had not yet identified whether other information channels were more effective in drawing the attention of the Abwehr (German military intelligence) or backing up a deception story. In contrast,

the Royal Navy ploy discussed earlier to lure Luftwaffe attacks against a decoy battleship in a 1942 Malta convoy was effective in part because British agents had fed relevant information to the Abwehr in advance. See Howard, *Strategic Deception,* p. 224.

77. Vego, "Operational Deception in the Information Age," pp. 61–62. Of note, a highly centralized decision-making architecture may be more vulnerable to exploitation. See Solomon, "Defending the Fleet from China's Anti-ship Ballistic Missile," p. 20.

78. Monte Carlo modeling and simulation might be able to inform such war gaming, but human players representing adversaries are needed to make decisions on the basis of scarcities, campaign priorities, and psychological intangibles, to have confidence in the findings.

79. JP 3-13.4, pp. II-1–II-3, IV-10–IV-11.

80. Holt, *Deceivers,* p. 94.

81. For example, Allied radio deception during World War II was centrally controlled by theater commanders and overseen by strategic deception-planning staffs in Washington and London. See ibid.

82. Vego, "Operational Deception in the Information Age," pp. 64–66.

83. For an example of this kind of analysis, see Kenneth S. Blanks [Capt., USA], "An Effectiveness Analysis of the Tactical Employment of Decoys" (master's thesis, U.S. Army Command and General Staff College, 1994), pp. 59–73. The modeling and simulation Blanks describes focus on tank decoys, but the basic issues are extensible to warships and aircraft.

84. For examples of U.S. Navy Cold War–era exercises used for this purpose, see Dwyer, *Seaborne Deception,* pp. 128–29, and Angevine, "Hiding in Plain Sight," pp. 81–84, 86–88.

85. Marshall Hoyler, "China's 'Antiaccess' Ballistic Missiles and U.S. Active Defense," *Naval War College Review* 63, no. 4 (Autumn 2010), pp. 84–105.

86. Though network-centric warfare is often described as inherently enabling decentralized operations, in the author's experience this has not uniformly been the case. Force commanders have often been tempted to control over-the-horizon subordinate units tactically and in real time using solely a displayed common situational picture. Aside from the fact that this picture has sometimes not been "common," let alone current, owing to technical limitations, the future cyber-electronic operating environment suggests that this degree of control will be increasingly difficult, if not impossible, to achieve.

87. See Peter Schweizer, *Victory: The Reagan Administration's Secret Strategy That Hastened the Collapse of the Soviet Union* (New York: Atlantic Monthly Press, 1994), pp. 6–8, and David Alan Rosenberg, "Process: The Realities of Formulating Modern Naval Strategy," in *Mahan Is Not Enough: The Proceedings of a Conference on the Works of Sir Julian Corbett and Admiral Sir Herbert Richmond,* ed. James Goldrick and John B. Hattendorf (Newport, R.I.: Naval War College Press, 1993), pp. 161–62.

88. For instance, exercises OCEAN SAFARI and MAGIC SWORD NORTH '81 "elicited probably the most extensive reaction from Soviet naval forces in almost a decade" and provided "an ideal opportunity to . . . assess the Soviet capability to conduct surveillance and target allied maritime forces." *Commander Second Fleet Calendar Year 1981 Command History,* box 234, Operational Archives Branch, Naval History and Heritage Command, Washington, D.C.

89. *Joint Operational Access Concept,* pp. 18–19.