SYM-AM-24-107

Excerpt from the Proceedings

of the

Twenty-First Annual Acquisition Research Symposium

Acquisition Research: Creating Synergy for Informed Change

May 8–9, 2024

Published: April 30, 2024

Approved for public release; distribution is unlimited.

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

Disclaimer: The views represented in this report are those of the author and do not reflect the official policy position of the Navy, the Department of Defense, or the federal government.

Acquired and Deployed but Not Adopted: Lost Mission Effectiveness Without Resilient Chat Afloat

Christopher B. Landis— is an Active Duty Commander in the U.S. Navy serving as a computer science PhD candidate at the Naval Postgraduate School. Upon graduating, he will report to the U.S. Naval Academy Cyber Science Department as a Permanent Military Professor. His education includes a BS in information technology with a second discipline in space operations from the U.S. Naval Academy and a Master of Information Technology Strategy from Carnegie Mellon University. He has served as a Surface Warfare Officer and Information Professional Officer, including three ship's company tours on a Destroyer, Littoral Combat Ship, and Aircraft Carrier. [clandis@alumni.cmu.edu]

Joshua A. Kroll— is an Assistant Professor of computer science at the Naval Postgraduate School. His research interests include trustworthy AI, technology governance, systems engineering, privacy, security, accountability, ethics, computer science and law, human factors, formal methods, data science, bias and fairness, dependability, and assurance. His education includes an AB in physics and mathematics from Harvard College and an MA and PhD in computer science from Princeton University. He has worked in both industry and academia. [jkroll@nps.edu]

Abstract

The U.S. Navy increasingly emphasizes communications resilience in distributed maritime operations. In the face of communications degradation and denial, we can improve warfighter effectiveness even using current systems when they are underused. By developing better ways to use deployed systems and applying lessons learned to new systems, we can maximize the value of system requirements and adoption of future acquisitions. Through our work on Navy communications systems' configurations, we find that some resilient systems go underused in practice, despite Navy requirements for system resilience designed into deployed systems. The Navy depends on Internet Protocol networks for conveying command and control (C2) communications. We examine the Navy's email and chat use for conveying C2 communications. We survey (n = 69) command, control, communications, and computer (C4) leadership to inform a sociotechnical analysis of how Sailors afloat use chat, considering a distributed chat architecture's resilience benefits. To ensure that acquired technologies do not go underutilized, our research results lead us to conclude that solutions must be sociotechnical: better technology alone does not solve the problem of resilient communications. Without understanding the operating environment, including operators' and their leadership's motivations, new technology solutions can go underused, limiting the anticipated gain in mission effectiveness.

Keywords: IT adoption, afloat tactical networks, chat, failure transparency, command and control communications, social computing

Introduction

Communications are critical to modern C2 in the U.S. Navy. Although afloat Internet Protocol (IP) networks provide much of the communications paths enabling C2 afloat, the Navy underuses these deployed IP systems and does not configure them to maximize their robustness in communications-degraded/denied environments (CD2Es). We offer a novel interdisciplinary approach to investigating how to overcome the organizational and technical hurdles in improving resilience in deployed capabilities. If we fail to understand why deployed systems go underutilized, we risk falling short in the same ways when investing in any future capabilities.

The U.S. Navy multiplexes a ship's multiple networks bidirectionally over multiple satellite communications (SATCOM) paths, interconnecting ships and fleet network operations centers (NOCs) ashore, as shown in Figure 1. An underused benefit of this architecture is its ability to interconnect ships without a shore facility (Landis, 2016). Combined with ship-hosted network services, any group of ships that can exchange IP traffic can use each other's services. However, the standard practice is to route all IP traffic via a NOC ashore, making the NOC a single point of failure. Why does the Navy not use existing shoreless capabilities to increase the resilience of applications conveying C2 communications?

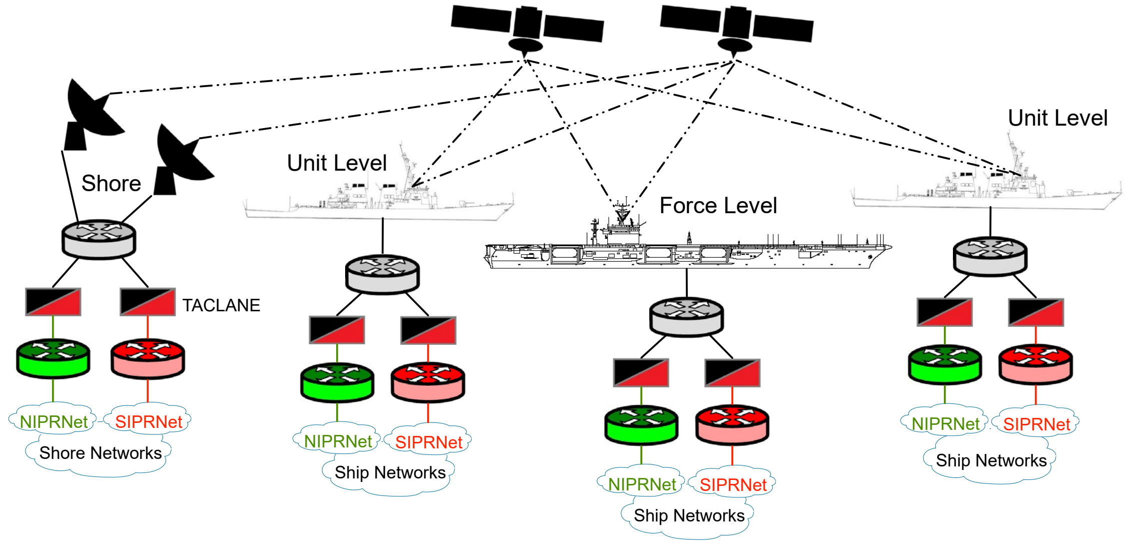

Figure 1. Conceptual Overview of Fleet Connectivity.

Note: The Navy primarily conveys unclassified communications over the Non-secure Internet Protocol Router Network (NIPRNet) and C2 communications over the Secure Internet Protocol Router Network (SIPRNet).

To answer this question, we investigate two IP network applications commonly used for C2 communications, email and chat, including their dependency on the Domain Name System (DNS). While we find technical reconfigurations may suffice for improving the resilience of email and DNS, such technical reconfigurations are insufficient for chat. We administer a survey of current and former afloat command, control, communications, and computers (C4) leadership, including embarked staffs, as part of our analysis of chat use. The survey data reveal that the most significant hurdles to using the afloat chat server include awareness of its existence, capabilities, benefits, and how best to use it. By combining our technical analysis with the results of our survey, we establish a base from which to derive interventions for improving Sailors' use of these systems. These interventions include caching all ships' DNS records on all ships, configuring fail-over or fault tolerance into ships' Exchange servers, and circulating a fleet commander-level championed how-to guide for operating a distributed chat architecture. We recommend circulating the guide as a means to overcome the structural obstacles that we find in the survey data for operating a distributed chat architecture. Enabling these applications to interconnect in a shoreless or otherwise CD2E and empowering Sailors to use these capabilities further the concept of assured C2 in distributed maritime operations, thus improving warfighting effectiveness.

Resilience relates to the concept of *failover transparency*, that the network status and configuration is transparent to the applications depending on it for connectivity (i.e., the application's logic need not depend on the network status in order for the application's function to survive degradation or failure at the network level). For instance, for chat, users' chat clients continuing to function despite their ship losing its connectivity with shore stations. Obviously, chat communications will be unavailable between ship and shore; but the point is that users aboard the ship will continue to stay synchronized with one another, retaining the ability to exchange messages despite the loss of shore connectivity.

We review both the social and technical contexts in the Stuck in One's Ways and Technical Context sections before addressing the data involved in our analysis in the Fleet Perception of Shoreless Chat section. We explain devised interventions in the Interventions and System Developments section and conclude our remarks in the Conclusion.

Stuck in One's Ways

Understanding why a technology is not being used to its fullest capabilities requires examining both the social context and technical aspects of the systems. In improving failover transparency in a shoreless environment for C2 resilience, the challenge is more than Sailors' capabilities on one ship. Instead, the configurations' complexity drives their implementation to the level of inter–program of record (POR) cooperation. As one person at this level, a former Naval Information Warfare Systems Command (NAVWAR) commander declared, "We have got to . . . turn CANES [(Consolidated Afloat Network and Enterprise Services)] into the information warfighting platform" (Machi, 2018). But technology is only part of the solution. Even when PORs cooperatively provision all the technical aspects well, people still must operate the system proficiently for it to yield its benefit to the Navy's mission.

When introducing the Naval Tactical Data System (NTDS), the Navy trained Sailors to be the system experts rather than relying on vendor technical support (Boslaugh, 1999, p. 254). This empowered Sailors to cross the boundaries between the multiple vendors supplying NTDS components. Today, being system-of-systems experts is important for Sailors to maximize their use of deployed information systems (ISs). Improving mission assurance through well-prioritized traffic flows of afloat network applications from various PORs is best achieved when including user behavior in the analysis (Rambo, 2016). Our work builds on this toward achieving greater resilience of a high priority traffic class, C2 communications. We find that with configuration refinements to afloat DNS and email and overcoming structural obstacles, the fleet will be in a better posture to assure its C2 communications paths.

A status quo bias emerges when uncertainty in the outcome of a policy change exists (Fernandez & Rodrik, 1991). This behavioral principle also applies to cybersecurity in which policy makers and practitioners alike are uncertain of the outcome of a change in policy because of the complexity of the cyber domain or a lack of understanding in how the policy change will affect how systems react at the technical and operational levels. Like information technology (IT) practitioners, builders—Sailors can be either of these—are in the class of trained professionals that often take pride in their work. Researchers studying hindrances to the adoption of innovative and sustainable technologies in the building industry discovered that psychological factors significantly affect companies' policy decision-making (Hofman et al., 2022). A lack of information transparency functions as a barrier to adopting new methods. When builders lack the information available to them that explains why a policy change or new technique is being introduced, they are more likely to stick to their traditions. If the explanatory information is available but difficult to find, the inconvenience of searching for and processing the information exacerbates their status quo bias. In cases like this, information transparency serves as a counterbalance to builders' resistance to change, often (if well justified) persuading builders even to embrace the new policy or technique (Hofman et al., 2022). Our survey data indicate that Sailors in the role of IT practitioners and users lack the prerequisite information about operating distributed chat architectures and their benefits. This deficit has led to their IT nonuse, corroborating this finding from the building industry as relevant to adopting IT.

Another question is whether a new system should adapt to existing processes or the processes should adapt to the new system. In neglecting to adapt its C2 communications to the full capabilities of a distributed chat architecture, the Navy has lingered in merely using basic chat functions, costing the Navy in the resilience that it could have been enjoying (Eovito, 2006). The Navy must adjust the technology's *metastructure*. Orlikowski et al. (1995) define metastructuring as:

> an empirically-grounded framing of the influential actions taken by individuals when they deliberately adapt computer-mediated communication technologies and their use to particular contexts and change those contexts to accommodate use of the technology. (p. 424)

Metastructuring can serve as an explanatory model in post-facto analysis or as an organization's approach to influencing its members' IT adoption. For example, in adopting a new enterprise resource planning (ERP) tool, Apple first tried to adapt the ERP tool to its existing workflows. When Apple Chief Executive Officer (CEO) Steve Jobs heard that this effort had become too expensive and cumbersome, he took a risk, directing Apple to cut its losses and start over, this time adapting its workflows to the new ERP tool, anticipating correctly that Apple would find greater success (Wipfler, 2023). An organization's metastructuring approach to adopting new IT affects the organization's success, including how clearly it communicates its goals, requirements, and risk tolerance (*reinforcement*) and incorporates new rules and procedures in response to user feedback as minor (*adjustment*) or major changes (*episodic change*; Orlikowski et al., 1995). Our analysis indicates that a lack of such organizational metastructuring has affected Sailors' nonuse of deployed systems.

Technical Context

The current ability of DNS, email, and chat to failover transparently when shore facilities are unreachable depends on having IP connectivity and the right configuration in place before the network interruption. Any multiplexed IP path between ships can contribute to the afloat network architecture shown in Figure 1, including a Ciphertext Time-division multiple access (TDMA) Interface Processor (CT-TIP) supernet, Battle Force Tactical Network (BFTN), and commercial proliferated low-Earth orbit (pLEO) networks. Transparent failover of these applications in a CD2E furthers the concept of distributed maritime operations. We address DNS, email, and chat in turn.

DNS Afloat

For users on one ship to connect directly with other ships' applications, their terminals must resolve the other ships' services' names to IP addresses. For example, remembering to connect to chat.c3f.navy.smil.mil is easier than remembering 205.3.33.20.[1] DNS is the service on which so much of the Internet depends. When connected to the NOC ashore, ships' DNS servers recursively query their servicing NOC's DNS server for any off-ship resource. Caching other ships' DNS records locally overcomes an unreachable shore but is not the current

[1] This IP address is fabricated for illustration only.

configuration. The fleet-wide DNS records are only in the four fleet NOCs.[2] To circulate and dynamically update fleet DNS records, all reachable services must be registered in the servicing NOC's DNS server and the server must allow zone transfers to ships. When ships are connected with their servicing NOC, ships' DNS servers should request zone transfers from the NOC periodically and automatically so that ships can operate without connectivity ashore. In turn, afloat DNS can support other applications without connectivity ashore.

Instead of caching all ships' DNS records on all ships, another option is to extend DNS with Service Location Protocol (SLP) adapted for ad hoc networks (Koubaa & Fleury, 2001). This would be more dynamic for a subset of interconnected ships; however, SLP incurs a delay in discovering services before applications can connect. Also, the Navy's strict configuration management generates an a priori knowledge of ship configurations that is simpler to implement manually by the POR upon system installation than by dynamic service discovery.

Email Afloat

The Navy conveys non-real-time C2 communications among commanders and staffs via email. Ships' email servers deliver all non-local email to their servicing NOC's email relay server (Landis, 2015). Once fleet-wide DNS records are available aboard each ship, improving email resilience becomes a configuration change. Enabling shoreless email requires reconfiguring ships' email servers to deliver directly to other ships when the NOC is unreachable. The Navy could improve transparent email delivery failover by one of two methods, of which both depend on having other ships' DNS mail exchange (MX) records: via multiple MX record preference levels or Exchange send connector costs.

MX Record Preference Levels

Using the basic fail-over capabilities of DNS, each ship's DNS records could consist of a lower-numbered preference (primary) MX record for the NOC and a higher-numbered preference (alternate) for its own email server, as listed in Table 1. Reportedly, 44% of about 2 million popular email-receiving domains use MX balancing or fail-over (Ruohonen, 2020). As a limitation to this approach, though, Ruohonen notes that this fail-over mechanism's lack of formal specification can yield differences in interpretation and behavior (Ruohonen, 2020). Notwithstanding, following strict configuration management—like the Navy's—can enable consistent results.

Table 1. DNS MX Record Fail-over Configuration; Lower Numbers Indicate Stronger Preference

Name	Type	Preference	Exchange
ship.navy.smil.mil	MX	10	mail.noc.navy.smil.mil
ship.navy.smil.mil	MX	20	mail.ship.navy.smil.mil

Exchange Send Connector Costs

Using the Exchange connector "cost" attribute, we can provide "fault tolerance" in email delivery (Ashalyengar21 et al., 2023). The principle behind these cost-adjusted send connectors, listed in Table 2, are these two rules:

[2] For security and better management of ships' bandwidth utilization, the Navy implements a *split horizon* DNS configuration such that all ship records resolve to the NOC when queried from outside the fleet boundary. As such, NOCs' DNS servers serve as ships' start of authority (SOA).

1. If a ship's email server can establish a Simple Mail Transfer Protocol (SMTP) connection with its servicing NOC, then deliver the email there for forwarding.
2. Else, try establishing an SMTP connection with the destination email server, identified by its MX record.

Whereas rule #1 is the only rule currently implemented (Landis, 2015), adding rule #2 would enable shoreless email delivery. Because ships' DNS servers would contain records only for the NOC and other ships, emails delivered by rule #2 would necessarily be destined for other ships. Other email would queue as normal until connectivity with the NOC ashore is reestablished.

Table 2. Fault Tolerant Exchange Connector Configuration

Address Space	Cost	Route Through or According To
*	10	NOC Email Relay Server
*.navy.smil.mil	10	NOC Email Relay Server
*.navy.smil.mil	20	MX Record for Recipient Domain

Note: Exchange will select the available connector with most specific address space with the lowest cost (Ashalyengar21 et al., 2023).

Chat Afloat

The Navy routinely conveys real-time C2 communications between tactical watch stations by chat. As such, the Navy has long required its chat capabilities between ships and shore stations to be resilient to CD2Es (Martin & Marcley, 2013). Eovito (2006) describes how a recommendation coming out of the U.S. Navy exercise Trident Warrior '04 to use distributed chat architectures subsequently became a Navy requirement and was tested during Trident Warrior '05. In this configuration, all afloat users connect their chat clients to their ship's chat server, whose channels are bridged with the servers on other ships or in the fleet maritime operations center (MOC) ashore, according to whoever owns the channel (i.e., fleet commander, strike group commander, etc.). When the ship loses connectivity with the shore, all shipboard users stay connected in the chat channels locally and can continue communicating with each other. Upon reconnecting with the shore, the channels automatically resynchronize the last pre-configured number of hours of history. Thus, a distributed chat architecture provides resilience for an unplanned, transient shoreless environment.

Curiously, Sailors do not use afloat chat servers in distributed chat architectures. Instead, users typically connect their chat clients only to servers ashore. This configuration is intolerant of network interruptions (i.e., all clients drop upon losing connectivity with the shore) and incurs additional bandwidth demand on SATCOM links with many afloat clients connecting ashore instead of a single server. Even if system administrators bridge afloat chat servers with off-ship servers, users still might not configure their chat clients to use their ship's chat server. Because enabling shoreless chat by a distributed architecture depends largely on afloat chat server administrators and end users' client configurations, we must understand them better, for which we offer our survey results in the Fleet Perception of Shoreless Chat section.

Our gap analysis yields different results depending on whether we frame our analysis within the Defense Acquisition Management System existing when the Navy acquired this software or today's Software Acquisition Pathway in the Defense Acquisition System's Adaptive Acquisition Framework. In the former system, the gap that we observe here occurs once the acquired chat capability reaches the operations and sustainment phase (Blanchette et al., 2010). The requirement owner (i.e., sponsor) did not reinforce the metastructure, that is, insufficiently championed the new capability and its benefits to fleet commanders such that Sailors do not use it in a distributed chat architecture. In today's terms, the Software Acquisition

Pathway prompts sponsors and program managers to interact with users continuously. Specifically, it directs the sponsor to assess annually "whether the mission improvements or efficiencies realized from the delivered software capabilities are timely and worth the investment" (DoD, 2020, p. 18). If followed, this feedback from end users to the sponsor and from the sponsor to the POR should prompt the fleet engagement necessary to expand the software's use because it reinforces and adjusts the chat system's metastructure (Orlikowski et al., 1995).

All ships had an Internet Relay Chat (IRC) server that can be configured to participate in a distributed chat architecture until April 2021 (*Mako 2.0: Administrator Guide*, 2021; *Mako 2.0: User Guide*, 2021) when an update of a third-party dependency broke the chat federation capability (D. H. Anunciado, personal communication, October 3, 2023). If anyone had been using the federation capability to effect a distributed chat architecture when that third-party's software updated, they certainly would have noticed its unexpected failure. Any complaints about losing the chat federation capability did not amount enough protest to demand an immediate replacement to provide that capability, which indicates its nonuse. However, the POR is working on testing and fielding solutions, including in the next version of ships' network services suite and with other chat software to integrate with newer communications capabilities. Any how-to configuration guide must therefore apply to newer chat software solutions.

Fleet Perception of Shoreless Chat

Of all the IP-conveyed C2 communications, tactical watch standers afloat most prevalently use chat. As described in the Chat Afloat section, using afloat chat servers to improve chat resiliently is not the norm. To discover why there seems to be little afloat chat server use, we survey current and former afloat C4 leadership, including embarked staffs (survey instrument detailed in the Appendix).[3] The responses help us discover the organizational and technical factors hindering Sailors from using their ships' chat servers. We find that Sailors are unaware of the server's existence, capabilities, or benefits (as shown in Table 3) and conclude that greater information transparency could support the metastructuring of chat server configuration to help increase its resilient use. For example, a fleet commander–level awareness campaign would be informative and prompt greater use, improving resilience for C2 communications conveyed by chat.

Table 3. Reasons for Not Using Afloat Chat Servers, Stratified by Those that Had the Chat Federation Capability

Reason	Population *n* ⇒ %		Capable *n*
Unaware of Server's Existence	20/64	31%	14/20
Aware of the Server's Existence but Do Not Use It	32/43	74%	23/32
Unaware of Channel Bridging Capability	15/31	48%	10/15
Unaware of the Benefits of Its Use	11/31	35%	8/11
No Time to Receive or Provide Training on Its Use	9/31	29%	7/9
Dealing with Too Many Other Network Problems	7/31	23%	6/7
I Don't Know	5/31	16%	2/5
Unaware of How to Connect	4/31	13%	3/4

[3] We presented some preliminary results at the Institute of Electrical and Electronics Engineers (IEEE) 2023 Conference on Military Communications (MILCOM; Landis, 2023).

No Operational Need (in Shipyard)	1/31	3%	1/1

Information Professional (IP) officers fill most C4 leadership billets so we solicited survey responses from them. With installations of the current afloat network server suite architecture starting in 2013, the population for this survey is about 510.[4] We collected 69 survey responses from those that have served on a ship at the force level (52%) or unit level (48%, *n* = 63).[5] This sample size yields a 9.2% margin of error (±6 of 69) at a 90% confidence level. Most respondents (70%) started their afloat tour before the POR stopped supporting the chat federation capability so they would have had the opportunity to use it so we stratify the survey data on this attribute.

Sailors Are Not Using Afloat Chat Servers

The reasons for not using the afloat chat server vary, as shown in Table 3, but the most significant hurdles include awareness of its existence, capabilities, and benefits, indicating a lack of support for reinforcing the metastructuring of resilience features into accepted technical configurations and work practices. About 30% (20, *n* = 64) are unaware of afloat chat servers. Of those in C4 leadership positions that are aware of afloat chat servers' existence, about three-fourths (*n* = 43) do not use them at all. They are unaware of the benefits of their use and untrained on their capabilities. For example, four Combat Systems Information officers (CSIOs) and a command, control, communications, computers, and intelligence (C4I) officer (P7, P34, P42, P45, and P55) report an apparent lack of benefit, one not knowing about the bridging capability. "I wouldn't want to add another chat capability separate of the existing C2 chat rooms used by FLTCDRs [(fleet commanders)] and units. I'm not sure what purposes this chat server will serve" (P7). "Even when I educated staff members about it, they wouldn't use it. The customers didn't know of bridging chat rooms to site [*sic*] that as a requirement nor did any of the ITs onboard know how to do that" (P34). As explained in the Chat Afloat section, a distributed chat architecture would improve the resilience of real-time tactical C2 communications. For every nonuse reason, except "I don't know," between 67% and 100% of participants had the chat federation capability, meaning they could have used it.

Responses to open-ended questions in our survey instrument reveal qualitative narratives for the sources of nonuse. Two participants (P20 and P29) ascribe Sailors' nonuse of afloat chat servers to requirements and culture.

Requirements

Chat requirements appear to have endured without a champion because the Navy treats the chat function more like a feature of existing programs rather than its own POR.

P29 claims that Sailors do not fully understand the *operational* capabilities of ships' networks, like the chat server, because no formal introduction to them exists. To make the point, P29 uses the example of the SharePoint server, which is online upon completion of the network installation but not configured or its operation introduced to the Sailors responsible for maintaining the network and its servers. The SharePoint home page not being unique for the ship does not prevent the server's use. But to get the most out of the tool in its operational

[4] Assuming a 10-year linear growth in installations to 170 ships, synchronized biennial officer transfers, and an average of 1 IP officer per ship, some ships having none and others several. With 6.25% annual attrition, we estimate a population size of approximately 435 of the 510 officers are available to survey in 2023.

[5] The *n* value for each question varies due to branching and each question's voluntary nature, enabling participants to skip some questions and quit the survey at any time.

context, Sailors must configure the system relative to that context. P45 concurs: “Likely wouldn’t have used it, as it would have likely not been configured and Sailors are not adequately trained to configure these servers without guidance.” This is akin to the lack of information transparency described in the Stuck in One’s Ways section in that Sailors do not have the requisite information to configure and operate chat afloat resiliently. Further, this finding echoes a Government Accountability Office (GAO) finding involving IT nonuse in the U.S. Immigration and Naturalization Service (INS) in which the report blamed a lack of training (GAO, 1988).

One need not look far for the root of this. All the Navy training courses for afloat computer network administrators listed in the Catalog of Navy Training Courses (CANTRAC)[6] share the goal of providing “the necessary knowledge and skills to perform advanced level networking system management, administration, and maintenance support,” or similar, in their descriptions. As such, Sailors responsible for managing, administering, and maintaining the network do not necessarily have the familiarity to operate all the services and software on its servers. For much of the specialized software—e.g., medical records software—expecting Information Systems Technicians (ITs) to be proficient in its operation is unreasonable. As another specialized software product, the Global Command and Control System–Maritime (GCCS-M) POR overcomes this problem by having three training courses: system administrator, operator, and watch officer. Although establishing a whole course on operating chat would be excessive, the Navy must increase Sailors’ awareness of distributed chat architectures and their benefits. Perhaps a one-page how-to guide on configuring and using the afloat chat server in a distributed chat architecture would be a more efficient and worthwhile approach.

Following this line of thinking, one may conclude that other features of in-use systems go unused because Sailors are unaware of them or their *operational* capabilities. Operational needs—as understood by the Office of the Chief of Naval Operations (OPNAV)—drive requirements. The GCCS-M POR requires Sailors to have specific training based on the nature of their interaction with the system, or the training would not be funded. The requirement for a distributed chat architecture made it into afloat tactical networks but without the associated organizational focus (metastructuring) to use its capabilities for the resilience of the Navy’s C2 communications, perhaps because no chat POR champions or oversees its use.

As a counterpoint, consider that a lack of capability requirements has not always hindered Sailors’ innovation attempts. For example, in 2011, before the Navy used dynamic multiplexing in its afloat IP connectivity, Sailors cross-connected SATCOM links based on typical throughput demands to increase the available throughput for the ship (Johnson, 2011). Sailors were watching unused transport capacity on one SATCOM link waste away while suffering through congested throughput on another SATCOM link, so they innovated to overcome the issue and improved their communications resilience. In contrast, with chat, no perceivable problem arises until the ship loses connectivity with the shore and then, the focus is on restoring the ship’s connectivity, not analyzing how to configure an application to be more resilient. Resiliency is invisible yet critical. Less motivation exists for fixing something that does not appear broken.

Culture

An aircraft carrier (CVN) communications officer (COMMO) suggests that the root of why Sailors do not use afloat chat servers combines a risk averse culture and the inexperience of C4 leadership:

[6] Access is restricted to DoD common access card (CAC) holders: https://app.prod.cetars.training.navy.mil/cantrac/vol2.html

> The poor performance history of CANES and senior personnel's risk averse culture have prohibited creative problem solving or the introduction of new ideas. Why haven't more IW or IP officers advocated to use the local chat server and federate it with the Fleet's directed chat server? Simple. The current talent pool for IP DIVOs [(division officers)] and CSIOs is plagued with LATXFRS [(lateral transfers)] that are still figuring out how to be DIVOs or learning what IP is let alone the systems under their charge.[7] (P20)

Although this sentiment is unique among participants, the survey data do not contain any reports of in-use distributed chat architectures to contradict it, even among participants that claim knowledge of the capability. Further, P20's sentiment is consistent with literature on how structural uncertainty—caused here by inexperience—leads to undue conservatism because of the possibility for unknown, undesirable outcomes (Rowe, 1994). With greater experience, like P20 demonstrates having, comes greater understanding of the communications and network architectures, which reduces structural uncertainty and the perceived risk associated with innovating to improve resilience. Because the inexperienced officers described by P20 lack time in the field, any intervention to improve chat use must consider administrators' and users' limited time to learn, configure, and teach others about using chat more resiliently.

One may argue that people sometimes do not adopt a technology because they believe that its disadvantages outweigh its benefits (Norman, 2013), but our data do not contain any indication that any Sailor believes in any disadvantage of operating a distributed chat architecture.

In the Apple ERP example (described in the Stuck in One's Ways section), the implementation team was too risk averse to upend current processes for those that promised to be better. The new ERP had too much structural uncertainty. The CEO needed to intervene through restructuring to bring about the greater good for the organization. Overcoming these junior IP officers' inexperience to prevail over their risk aversion may similarly need a CEO-level champion, like a fleet commander, who can improve the afloat chat architecture's metastructuring. A person in this authoritative position can recommend or direct using distributed chat architectures and provide justification for their use, refined requirements to PORs, and how-to guidance to fleet users.

Inherent in our recommendation for an awareness campaign is the assumption that if C4 leadership know that afloat chat servers exist and that they can achieve a distributed chat architecture that is more resilient than the prevailing configuration in which all clients connect directly to the MOC's chat server ashore, they will use this capability. This assumption is a limitation of our recommendation. The only indication in the survey data that a ship might use its chat server in a distributed chat architecture is P65's claim: "I would have ensured the entire strike group would have pointed their chat clients to the server so that it could have been utilized even if cut off from shore." Ten other participants (P3, P16, P19, P32, P35, P38, P46, P62, P63, and P67) claim they would have used it for improving communications internal to the ship. For example, P32 claims the use would be "To allow for the internal watch stations on the ship to maintain text comms even when down IP services." As an alternative use, P67 claims, "I would have liked to be able to chat to personnel aboard the ship internally. Sometimes emails are too slow especially if I know they on the computer." In part, this is why our recommendation includes a fleet commander-level champion, to encourage adoption. If a fleet commander believes

[7] "IW" is short for Information Warfare, of which IP Officer Community is a part. Officers laterally transfer between career fields and one having done so recently is relatively inexperienced in the new field. A division officer is the entry-level job for a ship's company officer.

operating chat in a distributed chat architecture is a good idea for C2 communications resilience, it is more likely to happen.

On Those That Use Afloat Chat Servers

Although they comprise a minority, understanding how Sailors who use afloat chat servers do so is informative to expanding their use. We list these details in Table 4 on how Sailors use afloat chat servers, from the nine respondents (*n* = 69) reporting such use. We summarize the following results from the data:

- On ships that use their chat server most frequently, the survey participants do not use it.
- Each of the five participants that did not bridge their chat servers claims either to not know of the server's channel bridging capability or that they did not devote the necessary time to figure it out.
- P6 reports the only bridged configuration but describes using the chat server for coordinating troubleshooting efforts among maintainers on the ship, a purpose that does not benefit by a distributed chat architecture.
- Except for P2, P15, and P50, participants listed in Table 4 started their tours before the installed chat software stopped supporting the chat federation capability (described in the Chat Afloat section).

Table 4. Chat Server Usage Details for Sailors Who Report Using Their Afloat Chat Server (9 of 69 Respondents)

P	Ship Class	Sailors' Use	Participant's Use	Purpose	User Location	Bridged	Perceived Effectiveness
P15	DDG	Routinely	Did not use	Operational	On my ship	Unknown	Moderate
P50	LSD	Routinely	Did not use	Operational	On my ship	No	Moderate
P2	DDG	Routinely	Did not use	Unknown	Unknown	Unknown	Effective
P21	CVN	Occasionally	Did not use	Operational	On and off my ship	Unknown	Moderate
P64	CG	Occasionally	Just a few times	Operational and Administrative	On my ship	No	Moderate
P6	CVN	Occasionally	Occasionally	Administrative	On my ship	Yes	Marginal
P43	CVN	Just a few times	Did not use	Administrative	On my ship	No	Ineffective
P60	CVN	Just a few times	Routinely	Administrative and Social	On my ship	No	Ineffective
P1	CVN	Just a few times	Just a few times	Proof of concept testing	On my ship	No	Moderate

Note. Cited Ship Classes: Guided missile cruiser (CG); Aircraft carrier (CVN); Destroyer (DDG); Dock landing ship (LSD)

We still find a lack of awareness of the afloat chat servers' capabilities and benefits. These findings are consistent with the subset of participants whose ships do not use their chat servers.

Interventions and System Developments

The “adage that we design our military systems to the requirements of the last war, rather than to meet the needs of a future war” (Boslaugh, 1999, p. 355) applies somewhat differently today. For example, its POR designed the afloat network multiplexing architecture for the maximum foreseeable throughput achievable by SATCOM; however, commercially available pLEO SATCOM capabilities threaten to overload it, having grown much faster than expected. In other words, even when we try to forecast our needs for the next war, “disruptive” technologies can disrupt our best designs. As the Navy develops and deploys additional capabilities to improve C2 resilience, it should apply the lessons discovered in the survey data to maximize these systems’ resilience and use, even when facing the next disruptive technology.

Besides the one-time technical reconfigurations that we recommend in the Technical Context section, we recommend the Navy continue multiple existing lines of effort to improve the resilience of its C2 communications using existing systems. One of these efforts approaches the DNS and email shortfall that we describe but by detecting connectivity status and dynamically reconfiguring systems automatically, according to the current connectivity status. Either the one-time reconfiguration that we offer or this dynamic reconfiguring solution is viable. We posit, however, that the greater complexity inherent in dynamically reconfiguring systems at times of need (i.e., during a loss or restoration of connectivity event) carries greater fragility than maintaining the consistent configuration we offer in this paper.

Another of these efforts involves an engineering change request (ECR) to increase the number of IP paths through which ships can communicate on SIPRNet directly without having to route through a NOC ashore (Stoffel, 2018). This is a necessary step to improving the resilience of C2 communications and recommend expanding it to other network enclaves. Without this piece of the solution, distributed chat architectures afloat will still improve resilience but be limited by the afloat network architecture.

U.S. Navy engineers are developing Communications as a Service (CaaS) to enable an *anything over anything* capability. It enables encoding IP traffic for conveyance over paths not traditionally recognized as IP paths. For example, one CaaS server can convey IP traffic to another CaaS server in J-series messages over a tactical data link (TDL).

CaaS developers are integrating new chat software that uses CaaS for its connectivity into afloat networks. The capability promises to be more resilient than previous chat capabilities because of its ability to use many communications paths, not just native IP paths. Will this become yet another unused capability akin to the distributed chat architectures that the fleet first used in Trident Warrior 2005 (Eovito, 2006)? What metastructuring actions will the Navy take to help ensure its success? Learning from the lessons observed in Sailors’ (non)use of afloat chat servers, the Navy should ensure that Sailors—maintainers and operators—are aware of the new chat capability, its benefits, and how best to use it to apply those benefits to bolstering the resilience of C2 communications.

Conclusion

The U.S. Navy’s dependence on IP networks for conveying C2 communications requires its leadership’s intervention to use the full capabilities of applications to maximize their resilience. We analyze DNS, email, and chat and provide technical recommendations for each of their configurations—applicable to afloat tactical networks—for improving their transparent failover. We conclude that all ships should have all ships’ DNS records cached locally so that the system can support other applications when unable to resolve queries from the NOC’s server ashore. Improving the resilience of email (i.e., getting it to work) without the NOC’s email relay server requires implementing an MX record fail-over or a fault-tolerant send connector configuration on ships’ Exchange servers.

Effecting a distributed chat architecture requires both a technical configuration change and additional metastructuring of resilient chat as a capability, including a championed awareness campaign. Our survey (*n* = 69) of C4 leadership informs a sociotechnical analysis of why most Sailors do not use chat servers afloat and how some Sailors use them, bearing in mind the resilience benefits of a distributed chat architecture. Survey data reveal that the most significant hurdles to using afloat chat servers include awareness of their existence, capabilities, and benefits, and how best to use their capabilities, indicating a lack of metastructure reinforcement. Promisingly, the relatively new Software Acquisition Pathway in the Defense Acquisition System's Adaptive Acquisition Framework directs an annual assessment mechanism that forms the very structure to reveal gaps like this to sponsors (DoD, 2020). Raising awareness will involve providing greater information transparency into why ships have afloat chat servers and how to operate them in a distributed chat architecture by having a fleet commander-level champion promote their use and circulate guidance. This circular combination of receiving feedback and implementing it throughout the fleet comprise an effective metastructuring approach (Orlikowski et al., 1995). Whether the Adaptive Acquisition Framework's annual assessment mechanism will yield tighter links between development and use is the subject of future research.

Finally, we describe the relevant interventions and systems currently in development and limited deployment. The energy and excitement around a new system with all its whiz-bang shininess can effect a metastructure episodic change that shakes people out of their routines such that they are willing to try something different or invent new practices to get at the new capabilities in the new system, as was ultimately the case for the Naval Tactical Data System (NTDS; Boslaugh, 1999). None of the new systems in development to which we refer amass enough gain in capability to stimulate such an episodic change. We must therefore understand the whole-system context for adopting each new system into Sailors' complex sociotechnical ecosystem through metastructuring reinforcement and adjustment. As the U.S. Navy emphasizes C2 communications resilience in distributed maritime operations and communications-degraded/denied environments (CD2Es), exploiting current systems—for better ways to use them and to apply lessons learned to new systems—can help keep new systems from the same nonuse fate and improve warfighter effectiveness.

References

Ashalyengar21, American-Dipper, chrisda, DCtheGeek, mattpennathe3rd, Ajayan1008, v-albemi, Duncanma, get-itips, msdmaguire, balinger, & SharS. (2023, February). Send connectors in Exchange server. https://learn.microsoft.com/en-us/exchange/mail-flow/connectors/sendconnectors?view=exchserver-2016

Blanchette, S., Jr., Albert, C., & Garcia-Miller, S. (2010, December). *Beyond technology readiness levels for software: U.S. Army workshop report* (Technical Report No. CMU/SEI-2010-TR-044). Software Engineering Institute, Carnegie Mellon University. https://apps.dtic.mil/sti/citations/tr/ADA535517

Boslaugh, D. L. (1999). *When computers went to sea: The digitization of the United States Navy*. IEEE Computer Society.

Department of Defense. (2020, October). *Operation of the software acquisition pathway*. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/500080p.PDF

Eovito, B. A. (2006, June). *An assessment of joint chat requirements from current usage patterns* [Master's thesis, Naval Postgraduate School]. https://hdl.handle.net/10945/2753

Fernandez, R., & Rodrik, D. (1991). Resistance to reform: Status quo bias in the presence of individual-specific uncertainty. *The American Economic Review*, *81*(5), 1146–1155. https://www.jstor.org/stable/2006910

Government Accountability Office. (1988, April). *Immigration service: INS' technology selection process is weak, informal, and inconsistently applied* (Report No. GAO/PMED-88-16). https://www.gao.gov/products/pemd-88-16

Hofman, B., de Vries, G., & van de Kaa, G. (2022). Keeping things as they are: How status quo biases and traditions along with a lack of information transparency in the building industry slow down the adoption of innovative sustainable technologies. *Sustainability, 14*(13). https://doi.org/10.3390/su14138188

Johnson, E. (2011). USS Enterprise SHF cross-connect configuration increases allocated bandwidth by 100 percent. *CHIPS*. https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=2298

Koubaa, H., & Fleury, E. (2001). A fully distributed mediator based service location protocol in ad hoc networks. *IEEE Global Telecommunications Conference (GLOBECOM '01)*, *5*, 2949–2953. https://doi.org/10.1109/GLOCOM.2001.965968

Landis, C. B. (2015). Email queues can be a false indicator. *CHIPS*. https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=5930

Landis, C. B. (2016). A new era of afloat IP services. *CHIPS*.

https://www.doncio.navy.mil/CHIPS/ArticleDetails.aspx?ID=8349

Landis, C. B. (2023, October). Afloat resilience of IP tactical communications: Chat systems and sailors [DTIC citation AD1215296, restricted distribution].

https://milcom2023.milcom.org/program/restricted-technical-program

Machi, V. (2018). Navy beefing up at-sea enterprise network. *National Defense, 102*(772), 30–31.https://www.jstor.org/stable/27022127

Mako 2.0: Administrator guide [Restricted distribution]. (2021, April). PEO C4I.

Mako 2.0: User guide [Restricted distribution]. (2021, April). PEO C4I.

Martin, O., & Marcley, A. (2013, July). *Mako chat support* (Notice of Intent No. N66001_SNOTE_0007EFDE). NIWC Pacific. https://sam.gov/opp/08d1ade640cd6fba0a02462113dbc880/view

Norman, D. A. (2013). *The design of everyday things* (Revised and expanded). Basic Books.

Orlikowski, W. J., Yates, J., Okamura, K., & Fujimoto, M. (1995). Shaping electronic communication: The metastructuring of technology in the context of use. *Organization Science, 6*(4), 423–444. https://doi.org/10.1287/orsc.6.4.423

Rambo, M. B. (2016, September). *System of systems engineering and integration process for network transport assessment* [Master's thesis, Naval Postgraduate School]. https://hdl.handle.net/10945/50470

Rowe, W. D. (1994). Understanding uncertainty. *Risk Analysis, 14*(5), 743–750.

https://doi.org/10.1111/j.1539-6924.1994.tb00284.x

Ruohonen, J. (2020). Measuring basic load-balancing and fail-over setups for email delivery via DNS MX records. *2020 IFIP Networking Conference (Networking)*, 815–820. https://ieeexplore.ieee.org/abstract/document/9142814

Stoffel, A. N. (2018, April). *Automated Digital Networking System (ADNS) system design description (SDD) PT routing ECR-ADNS-00928* [Restricted distribution]. PEO C4I, PMW 160.

Wipfler, G. (2023, June). *2023 spring quarter graduation—June 16, 2023 (full)* [29:20–43:23]. https://www.youtube.com/watch?v=Xuw8zqsPRTQ

Appendix Afloat Chat Server Survey

We received Institutional Review Board (IRB) approval to conduct this survey and Navy Survey Office authorization with control number NSPM23.14, expiring June 14, 2025.

We solicited survey participants via the Navy IP Officer's milSuite page with cross-posts into IP Officer Teams channels. The solicitation advertised that the survey supports research on improving the resilience of C2 communications in afloat tactical networks for the purpose of helping the Navy overcome sociotechnical barriers to using capabilities inherent within fielded systems. With 5–15 minutes to complete, Sailors could take this survey once for each CANES ship in which they served in an IT leadership position. The questions are as follows:

1. Have you ever or are you now serving aboard a CANES ship? *An answer of "no" or "I don't know" to this question ended the survey.*
2. What is the date range in which you served aboard this ship?
3. What is that ship's class?
4. What was/is your job title aboard that ship?

The remainder of the questions involve branching so we illustrate this flow in Figure A1.

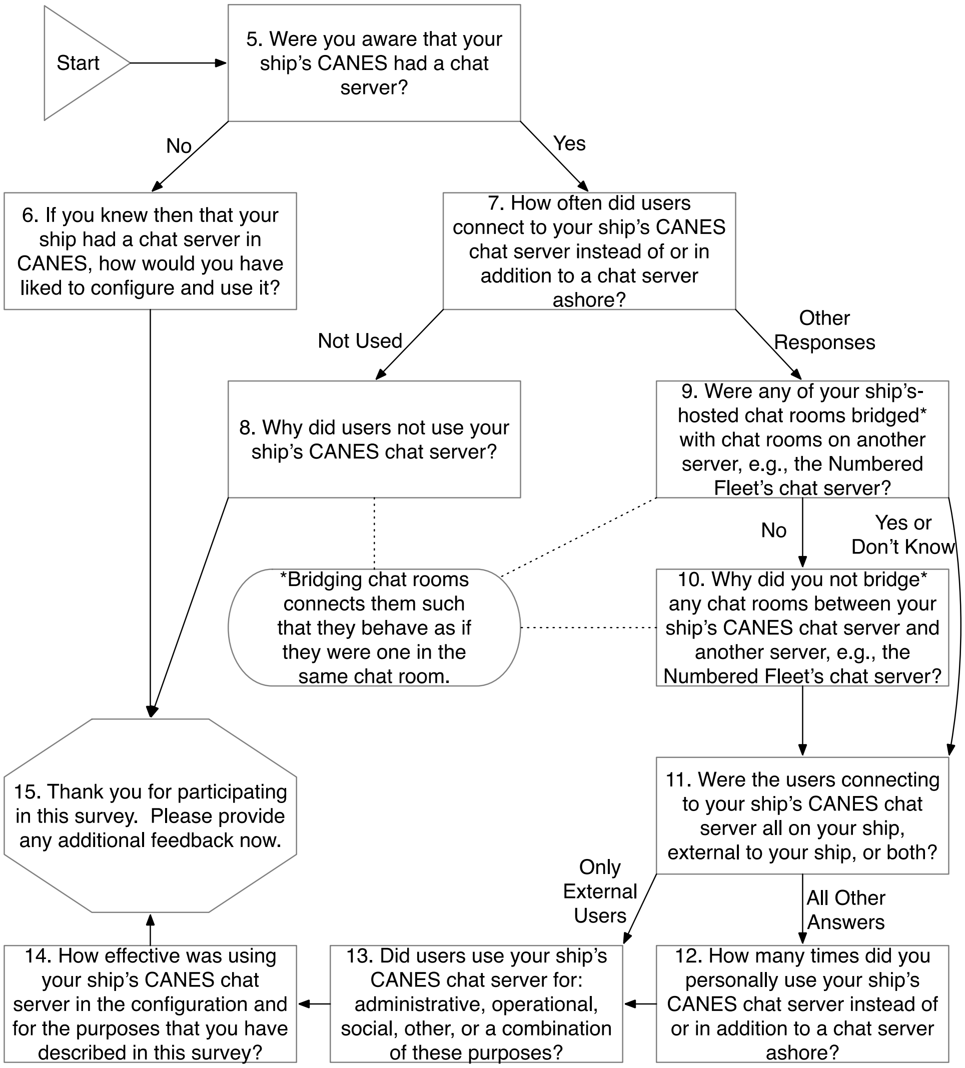
Start
5. Were you aware that your ship's CANES had a chat server?
No
Yes
6. If you knew then that your ship had a chat server in CANES, how would you have liked to configure and use it?
7. How often did users connect to your ship's CANES chat server instead of or in addition to a chat server ashore?
Not Used
Other Responses
8. Why did users not use your ship's CANES chat server?
9. Were any of your ship's-hosted chat rooms bridged* with chat rooms on another server, e.g., the Numbered Fleet's chat server?
No
Yes or Don't Know
*Bridging chat rooms connects them such that they behave as if they were one in the same chat room.
10. Why did you not bridge* any chat rooms between your ship's CANES chat server and another server, e.g., the Numbered Fleet's chat server?
15. Thank you for participating in this survey. Please provide any additional feedback now.
11. Were the users connecting to your ship's CANES chat server all on your ship, external to your ship, or both?
Only External Users
All Other Answers
14. How effective was using your ship's CANES chat server in the configuration and for the purposes that you have described in this survey?
13. Did users use your ship's CANES chat server for: administrative, operational, social, other, or a combination of these purposes?
12. How many times did you personally use your ship's CANES chat server instead of or in addition to a chat server ashore?

Figure A1

Chat Server Survey Questions 5–15

Acquisition Research Program
Department of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net