Mitigation Strategies for Communications Network Discontinuity for C2 in Tactical Environments

Kevin Chan
DEVCOM ARL, USA
kevin.s.chan.civ@army.mil

Paul Santry
Dstl, UK
psantry1@dstl.gov.uk

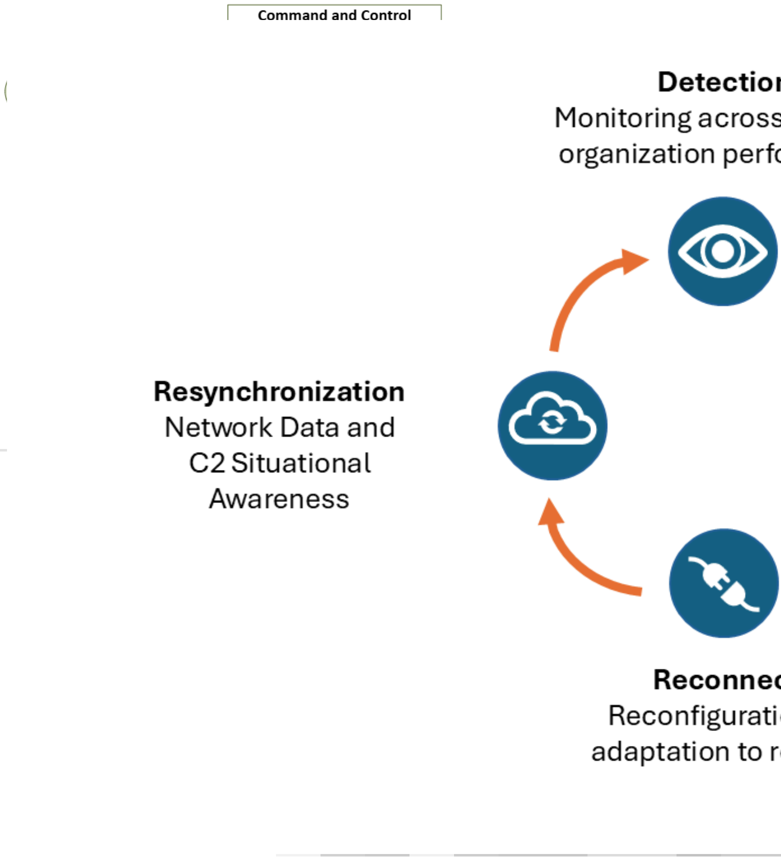
Thom Hawkins
U.S. Army PM Next Generation C2
jeffrey.t.hawkins10.civ@army.mil

Abstract

This concept paper surveys the critical issue of network discontinuity in tactical communications environments, where reliable connectivity is often compromised due to a range of adversarial, environmental, and systemic factors. As modern military operations increasingly depend on continuous communication for effective command and control (C2), understanding the causes and effects of network disruptions becomes paramount. Military networks operate in the denied, degraded, intermittent, or limited-bandwidth (DDIL) environment, which has the potential to severely inhibit network performance and subsequently C2 and associated C4ISR functionality. Commanders must anticipate some network discontinuity from adversarial, environmental, and/or systemic and technical causes. Techniques and policies can mitigate the impact of these network discontinuities. We explore the spectrum of these approaches and make recommendations for potential mitigation strategies in specific situations. This paper is divided into three sections. The first section reviews recent work on network discontinuity and C2 operating in DDIL environments. The second section proposes a framework in which to systematically consider network discontinuities, C2 and network mitigation strategies. The third section considers multiple use-cases on network mitigation for C2 and network performance. This paper provides insights on how to enable robust C2 despite a dynamic and contested environment and lessons learned on promoting such properties in operational settings.

1 Introduction

Command and control (C2) is a critical element to military operations and requires significant coordination within organizations. Without sufficient coordination, intended operational performance will be impacted and potentially interfere with other activities of the organization. Communications networking technologies are a critical enabling capability in multidomain operations, coalition or joint operations, or even within military organizations by providing valuable connections between organizing elements of a coordinated force. However, the tactical operating environment presents a dynamic and contested communications resulting in denied, degraded, intermittent, and limited-bandwidth (DDIL) communications environment [1] [2]. Network operators must devise methods to mitigate the impact of degraded communications and the downstream implication C2 performance and not be constrained by traditional C2 information flows. This concept paper proposes a closed-loop conceptual model that considers network mitigation strategies on degraded communications and subsequently C2.



As a motivating toy example, consider the case where a platoon leader must communicate their position every minute to their commander via tactical radio. The platoon is forward deployed and is located in an area with intermittent connectivity. There are cases where the reporting of position location information (PLI) is not successfully transmitted, resulting in delayed or inaccurate situational awareness of troop location and movement. This has potentially grave consequences. To overcome these challenges and mitigate the potential negative impact on various activities, one can envision a variety of technical or policy-based approaches. For example, the communications might have an alternate radio or method to communicate. Another approach is to communicate with another entity that has received delegation of authority to receive the PLI and has more reliable communications with the commander. The platoon may be operating under silence procedures; therefore, machine learning algorithms could be used to ascertain the likely position of the friendly platoon, i.e., last known position, likely movements considered by the artificial intelligence, with an output of likely position and reporting of dead reckoning area. This is commonly known as a primary, alternate, contingency, emergency (PACE) plan [3]. When each method of communications degrades below usable functionality, a next method is adopted. However, we will see that each approach may not be best suited for the circumstances whether the environment or mission or any other factor impose it.

This concept paper describes a closed-loop model comprising several concepts that characterize causes and effects on network discontinuity, its impact on network and C2 performance, and network mitigation techniques to enable sufficient network and C2 performance in cases where network discontinuities have occurred. Following the description of this method, we propose a systematic set of use-cases to test out the network mitigation strategies in the presence of network discontinuities across a complex network of C2 and technical communications.

1.1 Background

We consider the idea of network mitigation from a multilayer network approach in that we define two network layers (illustrated in Figure 1): the technical communications network and the C2 network. The communications network layer is deployed in support of the C2 network layer [4].

Un

As “there is no ‘one-size-fits-all’ approach to C2” [5], one must consider approaches to employ different ways to conduct C2. Based on a series of North Atlantic Treaty Organization (NATO) Science & Technology Organization (STO) activities, a C2 Agility approach was developed to understand how organizations can operate and then conduct C2 maneuver operations to switch to another C2 approach. One major finding of [5] described C2 agility of the organization to operate in a broad range of C2 approaches. Recent advances [6] [7] show a strong need for dynamically adaptive C2, so one must understand how to efficiently switch C2 approaches on the fly. These switches can be precipitated by a change in circumstances.

As the complexity of operations increase, heterogeneity is likely, both from a technical communications perspective and from a C2 perspective. For example, coalition operations will involve partners with a range of C2 agility, technical capabilities, and will have varying agreements with other partners. Any discord between C2 of participating partners or technical interoperabilitiy inadequacies may result in network discontinuities. Some combined, joint, or coalition partners may have advanced technical capabilities and operate with high C2 agility. As a result, more advanced coalition partners might have to operate with best endeavor with other partners. This may lead to C2 discontinuity when coordinating between the organizations. SAS-143 [7] describes these heterogeneous C2 situations as harmonization agreements. Allowing or designing networks to handle heterogeneity has strong potential for resilience and robustness against network discontinuity, but requires additional coordination both in planning and execution.

Our recent work has studied the causes and effects of network discontinuity in tactical network communications [1]. This served to fill a gap in the literature to understand technical reasoning for tactical networks “on what to expect and how to adapt with respect to operating on a discontinuous network” [1]. This work describes network discontinuity caused by adversarial influence, environmental factors, and systemic and technical causes. In this paper, we will additionally consider policy-based factors. These factors identify more downstream settings than just the technical aspects of the underlying communications network. However, a cross-layer network, which includes the organizational network adaptation approach, is potentially useful, as explored in [4] [7].

Similarly, Alberts [8] developed a risk mitigation framework that considers multiple aspects of the problem, including threats and hazards, remediations, extent and duration of the loss of cyber-enabled capabilities, restoration mitigation, and chains of consequence, consequence mitigation, cyber risk mitigation and cyber mission agility. Cyber risk also implies the presence of some adversarial entity. The approach recognizes the layered capability underscoring the complexity of the system. We claim that cyber is one contributing factor to the network discontinuity spectrum. This approach generalizes the impact of the threat and mitigation approach. We argue that the causes, effects and mitigation strategies can occur or be conducted at differing or various layers of this system.

Additionally, other NATO research activities have investigated adpatations to communications networks as a means to enhance agility and flexibility in tactical and coalition networks to overcome negative effects potentially caused by network discontinuities. These activities include: NATO STO Information Systems Technology Panel activities IST-194 Adaptive Networks at the Tactical Edge, IST-201 Federated Collaboration Services at the Tactical Edge and the use of AI/ML with middleware to improve digital throughput and IST-202 Federated Tactical Networks are conducting work in this area with IST-194 developing a novel network architecture with methods and protocols to adapt, manage, and control existing radio technologies in a heterogenous military network for increased robustness and optimized planning and 202 investigating Federated Mission Network Spiral 5 concepts and solution(s) for a federated network at the tactical edge. These activities focus on a single aspect of the space and we note the seeming lack of coordination of these capabilities and network policies in military policies. Previous work [1] can serve as an initial approach to formalize the concept; however, additional frameworks should be developed to formalize policies on providing assurance of the communications network in support of C2.

This concept paper considers an updated approach to the technical and policy mitigation strategies and describes several approaches under each of these categories and their implications on mitigating the negative impact of network and C2 performance.

2 Adaptation to Network Discontinuity

Adapting to network discontinuity is crucial in both maintaining communication effectiveness and minimizing the operational impacts of disruptions. Units should have a PACE plan for command, control, and communications in response to network discontinuity [3] [9]. This section outlines key adaptation processes, including detection, distinguishing between reversible and irreversible impacts, reconnecting the network, re-syncing data, and mitigating the effects of discontinuity through error correction and other techniques at the communications and C2 network layers. This is illustrated in Figure 2.

2.1 Detection of Discontinuity

The first step in adapting to network discontinuity is detecting when and where the network compromise happened. Soldiers often do not realize their communications through handheld devices (e.g., radios) are impacted. Detection can be made through monitoring tools that identify disruptions in real-time, such as sudden shifts in latency, packet loss, or drops in throughput. In adversarial contexts, detecting intentional attacks (e.g., jamming or signal spoofing) requires specialized intrusion detection systems. In non-adversarial scenarios, detection might focus on identifying environmental interferences or systemic failures, like signal attenuation over long distances. Effective detection is the foundation for initiating adaptive responses, as it enables the network to trigger pre-defined protocols (i.e., playbooks) for managing the disruption. Moreover, possessing protocols that span multiple network layers likely enhances the robustness and resilience of these systems to discontinuity.

Network discontinuity could be planned or unplanned and detection of these events is critical for mission operations. As an example of planned network discontinuity, a unit might cut connections to be clandestine or a unmanned aerial vehicle might travel beyond line of sight, or a mountain preventing any communications. In these cases, preplanning is necessary to delegate authority to the disconnected entities in the case where distribution of information and patterns of interaction among entities are degraded. In the context of C2 Agility [5], this is an example of operating “off the diagonal.” As a result, the preplanning must account for the time in which the entities are disconnected and also advance the mission despite not being connected. unplanned network discontinuity may be the result of some combination of adversarial, environmental, or systemic/technical causes [1]. Therefore, these systems must be able to detect these events and possibly execute adaptation of the network on multiple layers of the network to mitigate the impact of the discontinuity [1]. Such methods will have variable resource cost and detection accuracy.

Monitoring of multimodal information on the technical communications layer is another perspective on detecting discontinuities, with the Internet of Things (IoT) being a commonly cited example of this concept, where information from various modalities can provide diagnostics into the underlying network or system performance degradation [10, 11, 12]. These concepts can be included into PACE plans, and these plans can be incorporated into strategies to mitigate the impact or adapt to planned or unplanned network discontinuities.

2.2 Reversible vs. Irreversible Impacts

Once discontinuity is detected, one must assess the reversibility of impacts. Reversible impacts, such as temporary signal jamming, can often be countered through quick mitigation actions like frequency hopping [13], rerouting traffic [14], or deploying backup communication links [15]. Non-adversarial causes like environmental interference can be worked around using adaptive signal processing techniques or alternative routing strategies [16]. However, irreversible impacts, such as the destruction of critical infrastructure or permanent loss of bandwidth due to equipment failure, require more extensive recovery efforts, such as rerouting traffic through entirely new paths [17] or deploying replacement hardware [18]. Distinguishing between reversible and irreversible impacts is necessary to prioritize recovery actions and allocate resources effectively.

Impacts can be implemented on the C2 approach. For example, C2 agility suggests that with C2 maneuver, an organization can switch between multiple approaches, including edge, collaborative, coordinated, de-conflicted, and conflicted [5] [19]. These approaches are characterized by three operating conditions: distribution of information among entities, allocation of decision rights, and patterns of interactions [5] [6] [19]. The C2 Agility concept expanding upon the NATO Network Enabled Capability (NEC) [5] is shown in Figure 3. As a result, the organization can employ C2 maneuver as a reversible impact to the network to restore C2 in a degraded or denied environment [20]; however, because the system is quite complex, there is a need for understanding of the impacts of DDIL beyond “high,” “medium,” and “low.” C2 maneuver must also be done in coordination with the communications network.

From the technical communications network perspective, the network quality of service must be restored to meet the C2 requirement. One notable approach includes cross-layer adaptation and optimization for wireless networks which allows consideration of network configurations across multiple network functionality, such as routing and scheduling with the physical layer [11]. Managing the network layers concurrently expands the option space and the potential to overcome network discontinuities. However, Kawadia [21] cautions against extensive cross-layer adaptation approaches because it could lead to unintended negative consequences, routing loops, and difficulty in managing the added complexity. However, we note the distinction between adapting the overall complex network to restore C2 and adapting the overall complex network to restore communications connectivity. Fully restoring C2 or restoring C2 to meet the minimum requirements may not require fully restoring networked communications.

Temporary policies in information sharing or delegation of decision rights or decision-making represent reversible impact in the context of this paper. Other more enduring changes in policies of the same type of impact; however, one could consider organizational changes to evolve and not necessarily be irreversible. We can consider reversible impacts in the tactical environment as temporary event-driven adaptations that only last for a period of time within the mission, and we can consider irreversible impacts as those that are triggered by some event, and it is not expected that the organization will return to the original policy. Further, these enduring or temporary changes must not exceed mission requirements, or doing so might result in other unexpected issues [22].

An important aspect to consider, both from technical and policy-based decisions, involves the cost and resources required to implement the mitigation approach. In cases where the discontinuity is fleeting and short-lived, the correct approach may be to operate disconnected and in a degraded state for a short time until the discontinuity ends. In other cases, it might be useful to jointly consider network mitigation from a combination of technical and policy-based changes that involve understanding the relationship or “downstream” dependence of the C2 performance from any changes made on the communications network. We can also see how policy changes might impact communications network performance as well. For example, some information sharing policies might prevent entities from directly communicating, diminishing information sharing and situational awareness, but perhaps as a result of added security measures.

2.3 Reconnecting the Network

After detecting discontinuity and assessing the nature of the impact, the next step is to reconnect the network. In cases of temporary disconnection, reconnection may involve rerouting traffic through available backup links or shifting communication modes (e.g., from satellite to terrestrial radio) to restore connectivity. Rerouting of traffic might involve updating network management details, routing tables, and deploying additional nodes. In adversarial scenarios, this could involve countermeasures against ongoing attacks, such as signal spoofing or jamming, before re-establishing communication. Non-adversarial disruptions might require more straightforward reconnections, such as reconfiguring routers ([23]; [24]) or re-establishing line-of-sight in cases of natural obstacles [25]. The goal is to reestablish communications as quickly as possible while minimizing further disruptions.

Reconnecting the network on the C2 involves establishing communications between commanders and subordinates, potentially through alternate means, potentially involving command through alternate commanders or other communications mediums (e.g. PACE plans). For example, communications may be initially voice, but may have to switch to chat if tactical radios cannot support voice data requirements. Alternatively, speech-to-digital text capabilities, as being explored by IST-201, could be automatically introduced. This reconnecting approach is an example of semantic or cognitive communications, which aims to exchange the necessary information rather than just maximizing data transmission rates. A related concept is quality or value of information [26, 27] that aims to “get the right information to the right person at the right time” rather than just maximizing data rate or throughput. C2 can be conducted, in certain situations, with less information, communicate the same amount of information, but use fewer network resources.

2.4 Re-syncing Data Across the Network

Once the network is reconnected, it is necessary to resynchronize data that may have been updated at one node but not another. Discontinuity often results in incomplete, outdated, or inconsistent information being available across different nodes in the network. Re-syncing data ensures that all nodes have access to the most up-to-date information, which is especially important in systems where real-time data is crucial for decision-making. This process may involve resending lost packets, updating databases, or resolving conflicts in data versions that emerged during the period of disconnection [28]. Depending on the severity of the disruption, re-syncing can range from simple automated processes to more complex manual interventions requiring verification of critical data.

C2 data, specifically relevant to situational awareness, must be resynchronized and updated to reflect any information that changed during the discontinuity. Depending on the duration and severity of the disruption, the update will involve some amount of information exchange and validation of agreement across all situational awareness utilities. Policy is required to prioritise the data that is to be synced to ensure crucial data is delivered ahead of urgent or priority data in case of re-disconnection. Metadata (e.g., timestamps) are critical in order to ensure when re-connected, the ordering and recent of the data is understood and correctly reconstructued. For example, if PLI is synchronized incorrectly, then tracks might be indicating different movement.

A key example of resyncing data involves artificial intelligence or machine learning technologies that depend on current data to keep their models up to date. Data is often generated at the edge of a network, with proliferation of that data across the network occurring through a series of node synchronizations. DDIL constraints between one or more nodes or subnets may prohibit near real-time synchronization, an interruption compounded through data fusion and analysis requiring data sources from nodes across the network pegged to a particular timestamp. Data may be normalized (e.g., adhere to a schema, summarized) before transport across the network, which is sufficient for some uses. Machine learning, however, requires co-locating compute resources with extensive raw and/or historical data to train a model, even if the resulting model is relatively small. This means that either the data must be transported from the nodes where it is generated to centralized compute resources, or else compute appliances must be available at or near the network's edge to train a model locally. . These capabilities can be used at both the technical level to conduct some type of C4ISR applications, and they can also be used to support C2 functions.

2.5 Mitigation of Discontinuous Network Effects

Mitigating the effects of a discontinuous network involves employing techniques designed to maintain data integrity and minimize the impact on overall system performance. These techniques can be used both from a preventive approach to add passive robustness and resilience prior to deployment and from an adaptiveapproach that senses and reacts to discontinuitiy by reconfiguring the system or updating organizational execution of C2. The preventive measures potentially allow the network to maintain sufficient performance despite some adverse conditions, where without such measures, it would result in network disconnectivity. Alternatively, one can also consider dynamic adaptation techniques that require more reactive capabilities that sense the network disconnectivity and reconfigure some part of the system or organization to resolve the discontinuity.

2.5.1 Preventive/Passive

Preventive, passive mitigation strategies can be effective, providing built-in, safeguards to potential negative impacts. For example, error correction mechanisms play a significant role in recovering lost or corrupted data during transmission [29] [30]. These techniques are especially effective in both adversarial (e.g., jamming environments) and non-adversarial contexts (e.g., natural signal interference). Implementing adaptive QoS controls, such as dynamic bandwidth allocation [31] and priority queuing [32] can help manage limited resources and ensure critical data is prioritized. Other strategies include using data compression to maximize available bandwidth [33] and leveraging predictive analytics to preemptively address potential disruptions before they fully manifest [34] [35].

From a C2 perspective, PACE plans are a clear example of preventative planning, where coordination is required but the approach is passive in that the plan is agreed upon beforehand. This also relates back to mitigation of planned breaks in connectivity where an unmanned aerial vehicle that flies behind the mountain knows what path and other activities it should execute until it reappears and reconnects to the network.

2.5.2 Adaptive/Reactive

Network adaptation techniques are extensions to network optimization approaches, but employ run-time or online algorithms. Recent AI/ML advances include reinforcement learning and evolutionary algorithms. These approaches aim to maximize some utility function by adjusting network configuration, and the configuration converges to some maxima. These approaches can involve adaptation of network and application configuration to adjust to dynamic conditions [36]. On the C2 network layer, C2 Agility and C2 Maneuver capabilities address adaptive approaches to mitigating the negative impact of network discontinuities.

Adapting to network discontinuity requires a coordinated approach that begins with prompt detection, followed by a clear understanding of the reversible versus irreversible nature of the impacts. Successful adaptation then involves reconnecting the network, re-syncing disrupted data, and employing robust mitigation strategies to minimize the negative effects. By addressing each of these stages systematically, organizations can maintain operational continuity even in contested or degraded environments, ensuring that critical information continues to flow and supporting effective decision-making in the face of adversity.

3 C2 Network Mitigation Use-cases

In this section, we describe several operationally-relevant test-cases for network discontinuities and mitigation strategies. The examples are increasing in complexity and suggest a suite of experiments that could be run in lab settings or military test and evaluation experiments. They involve communications networks, C2 networks, and specific warfighting functions, and they can be used to understand the isolated and downstream impact of these mitigation strategies. The intent of this section is to communicate the critical importance of considering network mitigation in various scenarios, particularly as the operational environment or mission tasking increases in complexity (shown in Table 1. Description of Network Mitigation Use-Cases). It is suggested [37] that to ensure systematic testing of network discontinuity to use a a standardized set of use-cases that are relevant to the current world situation and that these tests should be performed in tactical networks (e.g., in support of Fires and Counterfires warfighting functions). Below is a progression of multiple use-cases in increasing complexity.

Table 1. Description of Network Mitigation Use-Cases

Use-Case	Nations Involved	National Domains Involved	Network Scale
#1	1	1	Small
#2	1	Multiple	Moderate
#3	Multiple	Multiple	Moderate
#4	Multiple	Multiple	Large

Use-case #1 involves a national domain where a platoon commander or forward unit encounters a viable target and requests for fire support from a supporting capability or capabalities (i.e., artillery). A first test focuses on initially constructing the baseline of a fully established network with no DDIL. Then each element of DDIL is implemented to measure the impact on the request for fires. Then the experiment can be run with network mitigation strategies (such as PACE) and attempt to perform the test.

Use-case #2 builds on Use-case #1 by having calls for fire originate from a capability in another national domain which will require hetrogeneous network policy alignment when DDIL effects are applied to the network (i.e., land from fires, air or space). Network discontinuity and mitigation strategies here can focus on multidomain network interoperability.

Use-case #3 again builds on the previous two use-cases and involves a nation receiving a call for fires from another nation. This use-case would involve international hetrogeneous partner networks, cybersecurity, and cross-domain guards which invoke and test international alignment of policies. The tests here would focus on interoprability across partner nations where policies and technologies are potentially incompatible.Network discontinuity and mitigation strategies here might focus on the challenges posed by policies of the involved organizations.

Use-case #4 studies the scalability of the solutions and understand the effectiveness of these approaches as the network grows in size. Network discontinuity and mitigation strategies here might focus on the challenges posed by policies of the involved organizations. These experiments might study the impact of large, heterogeneous networks and the ability to maintain synchronization of information and command in the presence of localized and or time-varying DDIL effects.

Each of these tests and the subsequent use-cases can be evaluated using various measures of performance (MoP) or measures of effectiveness (MoE) on which mitigation strategies enable effective performance of the use-case for a range of network discontinuities. The impact of the network mitigation strategies can be evaluated by measuring mission effectiveness, communications network performance, and C2 measures of effectiveness. These tests can also study the downstream effect of DDIL, comparing the relative impact of discontinuity and mitigation on the communications network and C2 layer. There may be situations where the communications network does not completely recover but the C2 layer is able to compensate [4].

4 Discussion and Conclusion

This concept paper describes a model for network mitigation strategies to counter network discontinuities in tactical networks. This work has identified a critical need to systematically understand the impact of network discontinuities on military operations and to also understand the impact that network mitigation strategies can provide in a wide range of situations. While there are technical and policy-based solutions, it is important that the testing and design of these concepts into systems and policies be considered in a holistic, systematic fashion.

Based on our awareness of NATO S&T activities, we suggest that a unifying strategy on how to combat DDIL impacts is needed. Currently, individual parties have their own strategy, technology and culture, which result in stovepiped organizations and capabilities. Military operations can be significantly enhanced with a coordinated multinational, multidomain operational force.

Experimentally, we see a great need for end-to-end experimentation to test and evaluate network migitation strategies for network discontinuities. While it is critical to understand how to provide robustness of C2 and communications in the presence of DDIL networking, we also need to understand the nuances of the performance of the network mitigation strategies and the impact on how to conduct C2 in the presence of these adpatations. Further, there may be cases where the adaptation is performed on the network layer and the C2 is unaffected and unaware but performance is maintained. If the existing mitigation strategies can keep up with the unplanned network discontinuities and the user is not affected, this represents the ideal case. Characterization of these complex interactions and adaptations is vital towards the management of the networks and setting of policies across complex organizations.

5 References

[1] T. Hawkins and K. Chan, "Causes and Effects of Communications Network Discontinuity in a Tactical Environment," *The International Conference on Military Communication and Information Systems (ICMCIS),* Apr 2025.

[2] P. Santry, "Military Communications Information System Definitions and Policy White Paper (DSTL/CP157645 v1)," Defence Science and Technology Laboratory UK, Porton Down, 2024.

[3] Center for Army Lessons Learned, "Handbook No. 18-28: Operating in a denied, degraded, and disrupted space operational environmen," June 2018. [Online]. Available: http://call.army.mil/. [Accessed 9 June 2025].

[4] K. Chan and D. Alberts, "Exploring Composite Network Agility," in *ICCRTS*, 2015.

[5] "NATO SAS-085 Final Report on C2 Agility, STO-TR-SAS-104," NATO, 2014.

[6] "C2 Agility: Next Steps (STO-TR-SAS-104)," NATO STO, 2018.

[7] "Agile Multi-Domain C2 of Socio-Technical Organizations in Complex Endeavors Operating in a Contested Cyberspace Environment (STO-TR-SAS-143)," NATO STO, 2024.

[8] D. Alberts, "Cyber Risk to Mission: Assessment Methodology (STO-MP-SAS-OCS-ORA-2020)," NATO, 2020.

[9] W. Coffey, J. Roussseau and S. Mudge, "Denied Degraded Disrupted," Jan 2018. [Online]. Available: https://purview.dodlive.mil/Home/Story-Display-Page/Article/2618088/denied-degraded-disrupted/. [Accessed 9 June 2025].

[10] A. Sheth, P. Anantharam and K. Thirunarayan, "Applications of multimodal physical (IoT), cyber and social data for reliable and actionable insights," in *10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Miami, FL, USA, 2014.

[11] X. Lin, N. Shroff and R. Srikant, "A tutorial on cross-layer optimization in wireless networks," *IEEE Journal on Selected areas in Communications,* vol. 24, no. 8, pp. 1452-1463, 2006.

[12] M. Wigness, T. Abdelzaher, S. Russell and A. Swami, Internet of Battlefield Things: Challenges, Opportunities, and Emerging Directions, Wiley, 2022.

[13] M. Liechti, V. Lenders and D. Giustiniano, "Jamming mitigation by randomized bandwidth hopping," *11th ACM Conference on Emerging Networking Experiments and Technologies (CoNEXT),* pp. 1-13, 2015.

[14] U. Patel, T. Biswas and R. Dutta, "A routing approach to jamming mitigation in wireless multihop networks," in *2011 18th IEEE Workshop on Local & Metropolitan Area Networks (LANMAN)*, Chapel Hill, NC, USA, 2011.

[15] W. Hreha, D. Grybos and R. Singh, "Commercial SATCOM communications protection: Commercial SATCOM resilience to jamming," in *IEEE Military Communications Conference (MILCOM)*, Baltimore, MD, USA, 2012.

[16] T. Hoang, R. Kirichek, A. Paramonov, F. Houndonougbo and A. Koucheryavy, "Adaptive routing in wireless sensor networks under electromagnetic interference," in *International Conference on Information Networking (ICOIN)*, Da Hang Vietnam, 2017.

[17] G. Kesidis, D. Miller and Z. Qiu, "IP-level Fast Re-Routing for Robustness to Mass Failure Events Using a Hybrid Bandwidth and Reliability Cost Metric," in *IEEE Military Communications Conference (MILCOM)*, Baltimore, MD, USA, 2016.

[18] R. Duffey, "Emergency Systems and Power Outage Restoration Due to Infrastructure Damage from Major Floods and Disasters," *INSIGHT,* vol. 23, no. 2, pp. 43-55, 2020.

[19] D. Alberts, R. Huber and J. Moffat, "NATO NEC C2 Maturity Model," NATO STO SAS-065, 2010.

[20] F. Bernier, K. Chan, D. Alberts and P. Pearce, "Coping with Degraded or Denied Environments in the C2 Approach Space," in *International Command and Control Research and Technology Symposium*, Alexandria, VA, USA, 2013.

[21] V. Kawadia and P. R. Kumar, "A cautionary perspective on cross-layer design," *IEEE Wireless Communications,* vol. 12, no. 1, pp. 3-11, 2005.

[22] U.S. Air Force, "AFDP 3-0.1, Command and Control,"

Air Force Doctrine Publication, 2025.

[23] F. Clad, S. Vissicchio, P. Merindol, P. Francois and J. Pansiot, "Computing minimal update sequences for graceful router-wide reconfigurations," *IEEE/ACM Transactions on Networking,* vol. 23, no. 5, pp. 1373-1386, 2014.

[24] E. Keller, "Refactoring Router Software to Minimize Disruption," Princeton University, 2011.

[25] M. Rahman, L. Bobadilla and B. Rapp, "Establishing line-of-sight communication via autonomous relay vehicles," in *IEEE MILCOM*, 2016.

[26] K. Chan, K. Marcus, L. Scott and R. Hardy, "Quality of information approach to improving source selection in tactical networks," *2015 18th International Conference on Information Fusion (Fusion),* pp. 566-573, 2015.

[27] C. Bisdikian, L. Kaplan and M. Srivastava, "On the quality and value of information in sensor networks," *ACM Transactions on Sensor Networks (TOSN),* vol. 9, no. 4, pp. 1-26, 2023.

[28] A. D'Atri, M. De Marco, N. Casalino, C. Cappiello and M. Helfert, "Analyzing Data Quality Trade-Offs in Data-Redundant Systems," *Interdisciplinary Aspects of Information Systems Studies: The Italian Association for Information Systems (Springer),* pp. 199-205, 2008.

[29] S. Kahkeshan and Z. Homavazir, "Enhancement of voice quality and system capacity by error detection and correction method in wireless digital communication," in *2023 IEEE 4th Annual Flagship India Council International Subsections Conference (INDISCON)*, 2023.

[30] J. Ababneh and O. Almomani, "Survey of error correction mechanisms for video streaming over the internet," *International Journal of Advanced Computer Science and Applications,* vol. 5, no. 3, 2014.

[31] J. Boley, E.-S. Jung and R. Kettimuthu, "Adaptive QoS for data transfers using software-defined networking," in *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, Bangalore, India, 2017.

[32] Z. Qiao, L. Sun, N. Heilemann and E. Ifeachor, "A new method for VoIP quality of service control use combined adaptive sender rate and priority marking," in *IEEE International Conference on Communication*, Paris, France, 2004.

[33] J. Liu, J. Huang, Z. Li, Y. Li, J. Wang and T. He, "Achieving per-flow fairness and high utilization with limited priority queues in data center," *IEEE/ACM Transactions on Networking,* vol. 30, no. 5, pp. 2374-2387, 2022.

[34] S. Jain, M. Khandelwal, A. Katkar and J. Nygate, "Applying big data technologies to manage QoS in an SDN," in *12th International Conference on Network and Service Management (CNSM)*, 2016.

[35] N. Ansari, C. Zhang, R. Rojas-Cessa, P. Sakarindr, E. Hou and S. De, "Networking for critical conditions," *IEEE Wireless Communications,* vol. 15, no. 2, pp. 73-81, 2008.

[36] J. Perazzone, M. Dwyer, K. Chan, C. Anderson and S. Brown, "Enabling machine learning on resource-constrained tactical networks," in *IEEE Military Communications Conference*, Rockville, MD, USA, 2022.

[37] K. Marcus, "Annex D – IST-124 EXPERIMENTATION EXECUTION (STO-TR-IST-124-Part-I)," NATO STO, 2019.

[38] M. Ryan, "A Short Note on PACE Plans," *Infantry,* p. 13, July-September 2013.