NATO COMMAND AND CONTROL CENTRE OF EXCELLENCE

NATO COMMAND
AND CONTROL CENTRE
OF EXCELLENCE
(NATO C2COE)

P.O. BOX 90004
3509 AA UTRECHT
THE NETHERLANDS
TEL: +31 30 21 87021

NATO C2COE REPORT

ANALYSIS OF COMMAND AND CONTROL ASPECTS DURING EXERCISE STEADFAST COBALT 2017

ON BEHALF OF THE NATO C2COE,

Renée van Pamelen-Hollenberg
Captain, NLD N
Director, NATO C2COE

Stephen Gray
Lieutenant Commander, USA N
Staff Officer, Analysis and Concepts Section, NATO C2COE

DISCLAIMER: This report is a product based on an analysis by the NATO C2COE. It does not represent the opinions or policies of North Atlantic Treaty Organization (NATO) or those of the nations sponsoring the NATO C2COE. It is designed to provide an independent opinion.

TABLE OF CONTENTS

CHAPTER 1 - INTRODUCTION

EXECUTIVE SUMMARY

The United States (U.S.) has participated in Exercise STEADFAST COBALT (SFCT) in previous years, but 2017 is the first year that the U.S. attempted confirmation in accordance with Federated Mission Networking (FMN) framework (Spiral 1.1 specifications). The NATO Command and Control Centre of Excellence (NATO C2COE) embedded with the United States European Command (USEUCOM) forward headquarters (HQ) element to analyze the command and control (C2) exercise element of SFCT 17, which is the Communications Exercise (COMEX) for TRIDENT JUNCTURE 18 (TRJE), and provide recommendations for improvement to make it a more effective and operationally relevant exercise. This report consists of observations, analysis, and conclusions made by the NATO C2COE during the exercise.

There are three major takeaways from the NATO C2COE's analysis. First, the focus of effort for SFCT should shift to preparation. All efforts to design, build, test, authorize, federate, and operate, etc. a Mission Partner Environment (MPE) instantiation[1] should be accomplished in garrison as much as possible. The goal of SFCT should shift to setting up, federating, and validating in the least amount of time, with the least amount of logistical footprint, at the least amount of cost, in a repeatable manner. All units involved have to train like they fight, and weeks of setup will not be an acceptable course of action during a contingency. This effort must be regularly exercised in garrison and at NATO exercises to develop the knowledge, skills, and abilities needed to execute quickly in a challenging operational environment.

Second, more focus on the operational perspective is needed to validate the systems built and tested at SFCT. Without operators descending on the exercise site in the last days to 'validate' the design, it is hard to say that it would meet the end user's needs. Stress testing (simulating the number of users and associated bandwidth requirements) is less relevant immediately, but operational scenario testing is. Questions like 'can my team of _____ amount of personnel use this network simultaneously?', 'can I share information with _____ and see their information as well?', 'can I talk to _____ using voice/video/data?', and 'can I reach back to my _____ system in garrison?' are all questions that require the J2/J3 perspective, and can be best informed by on site participation. Requirements that future mission partner environment networks should be secure, modular, flexible, scalable, deployable, sustainable, and interoperable are known. J2/J3 personnel should now make the operational requirements understood and codify them for every operational scenario. This will need to be quickly followed by additional efforts to ensure that administrative, logistic, planning, training, and other requirements that come from other portions of the staff are incorporated.

Finally, SFCT should represent the culmination of processes that are defined, tested, validated, exercised, and improved. Success in communications ultimately comes down to preparation. There should be written guidance developed for all configurations, especially those that are untested and unproven. This ensures that any communications provider (from any service component, including airborne and afloat platforms) could be provided the information

[1] While the term Mission Partner Environment (MPE) will be used in this report, it should be understood that this term is used to describe any national network that is FMN compliant that is meant to interconnect with other FMN compliant partners.

they need to make the configurations required (and possibly equipment available) in short order to give capability to the commander. Configurations should be built in accordance with FMN spiral specifications to ensure that the desired interoperability is not lost in the configuration management process.

There are many other important points discussed in the analysis that follows that goes into detail on the above topics and more. But, before concluding it is important to discuss the future. During the final distinguished visitor (DV) event at SFCT, there was an opportunity for senior NATO leaders to discuss what they had learned from the reports they had received during the course of the exercise and the information shared with them during the previous DV events. A common theme of concern among the feedback was that the SFCT exercise and the network was becoming increasingly complex. The number of units, personnel, hardware devices, software applications, diagrams, scenarios, and tests were significant, and had grown to be the largest in scope for any SFCT to date. So, the argument from the senior leaders was that the exercise should be adjusted so that it would become less complex. The NATO C2COE argues that instead of less complexity, what is actually desired by senior leaders is more clarity. Leadership needs to fully understand their capabilities, be able to execute them in a repeatable manner, with a responsiveness that achieves the advantage necessary to achieve mission success in a dynamic operational environment. The underlying complexity to achieve this will continue to grow, but the ease in which the commander should be able to understand and use their capabilities should only continue to improve, despite this. The SFCT exercise was focused on FMN confirmation using the Spiral 1.1 specification. Future specifications are only going to add more hardware, more software, more nations, more interconnections, etc. in an effort to achieve more streamlined interoperability among NATO, NATO nations, and other nations as FMN affiliates. Additionally, technological advances are bringing new capabilities to operational units at a quickening pace. Last year, Lieutenant General Lofgren, United States Air Force, Deputy Chief of Staff for Capability Development, Headquarters Allied Command Transformation said, “things like big data scare people and they don't understand it, artificial intelligence, cognitive computing, and federated clouds are thought to be science fiction but they exist today—they are real today. Early adopters will gain the edge and therefore NATO needs to take this step.[2]” Capabilities like Lieutenant General Lofgren mentions, plus some others like mobility, robotics, and unmanned systems that are already in use, were not integrated during SFCT. Additionally, SFCT did not incorporate the realities of an operational environment that would mean the forward headquarters would be under significant threat from various sources. So, given this, it should be expected that SFCT actually gets more complex, not less.

RESEARCH OBJECTIVES

The objective of this report is to advise USEUCOM, the NATO Command Structure (NCS), NATO Force Structure HQs, and nations, on C2 considerations for deploying forward mission partner environment instantiations in order to provide them with ideas for future use and to avoid re-inventing the wheel, repetition of effort, and repetition of mistakes. Its goal is to, where possible, determine the root cause(s) of observed issues during the exercise and identify the remedial action(s) that will address those root causes, in order to correct the problem or sustain the success, potentially leading to lessons identified and/or best practices.

[2] Kucukaksoy, I. (2016, July). NATO capability development and interoperability. *The Three Swords Magazine*. Retrieved from http://www.jwc.nato.int/images/stories/_news_items_/2016/LT_GEN_Lofgren_interview.pdf

BACKGROUND & CONCEPTS

The NATO C2COE's main mission is to provide NATO, nations and international organizations with support and expertise on specific aspects of C2 with a focus on the operational environment.

FACTORS AFFECTING THE ANALYSIS

There are several factors to be taken into account with regard to SFCT 17 and consequently the observations and recommendations made in this report. The primary audience observed during this exercise was the communications portion of the USEUCOM forward HQ element. This communications element was made up of various units, including augments from outside the theater, and does not necessarily represent the make-up of personnel that would conduct SFCT next year, or in an actual operational scenario. It also does not necessarily represent what would be observed from other entities operating at SFCT. As always, personal factors such as a personality, culture, experience, organization, etc. affect the outcome of the exercise and the observations made during the exercise. Other factors are limitations with regard to the resources available (financial, man-power, expertise), the physical limitations of the analysis team (only one individual), limitations of time (attendance only at the Technical Coordination Conference and the exercise evaluation period) and the fact that there is no (significant) room for experimentation. Moreover, the focus and goal of exercises such as this tends to be on certification as opposed to actual concept development.

STRUCTURE OF THE REPORT

The detailed findings and recommendations are delineated in a framework of 1) Observation(s) made and discussion of the issue(s); and 2) Conclusion(s) and recommendation(s). Where relevant, categorization of the recommendations is made by referencing the Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities, and Interoperability (DOTMLPFI) lines of capability development. Sections on execution and future concepts were also added for clarity.

CHAPTER 2 – OBSERVATIONS

ITEM 1: DOCTRINE	
1.1 Observation / Discussion	**Conclusion / Recommendation**
Joining, Membership, and Exit Instructions (JMEIs) were received late and still in draft form, which significantly slowed down setup of the mission network and caused rework to be required in some situations. Other network configurations, such as Internet Protocol (IP) space configurations, were not received in a timely manner and were implemented in a non-standardized, but ultimately successful way through direct interaction with other exercise participants.	Earlier receipt of documentation to include JMEIs and other network configurations is required. If the draft of this information could be available at the Technical Coordination Conference (TCC) and the JMEIs finalized very soon after, this would allow nations to implement a significant number of configurations ahead of time, considerably speeding up the process of getting communications set up at exercises and in support of actual operations.
1.2 Observation / Discussion	**Conclusion / Recommendation**
Continuity of Operations (COOP) planning should be a consideration during planning of setup of the SFCT network and footprint.	While it is somewhat unlikely that a full relocation of a forward HQ would be required, what is more likely is that there could be a loss of infrastructure services such as power or heating, ventilation, and air conditioning (HVAC), there could be significant weather impacts, or significant threat increase, loss or degradation in the communications path, or any other number of similarly scoped events. Of course, if this were an actual operation, adversary tactics and movements, air and indirect fire threats, and other eventualities would also have to be closely monitored to determine if the COOP plan should be implemented. Contingencies this COOP plan should consider should include all the way from prudent preparations like more frequent validation of backups and synchronizations, all the way to more robust preparations like standing up a full alternative hot site ready to take over operations in case of a significant disruptive event. With respect to a loss of degradation of terrestrial or satellite communications capability, alternate paths should be in place to ensure communications aren't lost if one path becomes degraded or denied. As with

	any COOP plan, training, standardization, and periodic exercising of the plan are essential for success.
1.3 Observation / Discussion	**Conclusion / Recommendation**
Gaining the Authority to Operate (ATO), the final step in a security certification risk management process, is essential, but the overall process needs to improve. Significant delay in ATOs are an unnecessary burden that prevents effective operations.	Initially, familiarization with the ATO process will allow it to go much smoother regardless of the system or classification level involved. Additionally, having a well-defined software configuration ahead of time will prevent the process from starting late. The ATO process won't be able to start until a software baseline is provided, so software changes should be avoided after the SFCT TCC. Additionally, ATOs require that a recent software vulnerability scan be conducted with the result provided. This means that not only does the network have to be built, but it also has to be able to pull patches from its vulnerability management source, scanned by an appropriate vulnerability management tool, and those vulnerabilities that are found have to be mitigated. Ultimately, putting this whole process into place allows all other processes that require system connection or inter-connection to start earlier. This process does not eliminate the necessary delay while the ATO request is being processed, but these efforts will keep that delay to a minimum.
1.4 Observation / Discussion	**Conclusion / Recommendation**
Standing plans associated with communications footprint requirements should be established and maintained. The overarching goal of these plans is to have as many communications capabilities that you need, can afford, can lift, can support, but not more, specified for any given size operation.	A communication footprint standing plan can be shared with entities that would provide the various logistic capabilities that are required, allowing for proper planning to be conducted. This plan also should be reviewed periodically to make sure the capability requirements still match with shifting operational requirements. This plan should also have associated readiness timelines, which allows service and equipment providers to appropriately plan for maintenance, acquisition, and other factors that may affect readiness. Beyond the logistics of communication capabilities, the equipment configurations should be as close to what will be required as well. Using a virtual data center (VDC) construct

	and deploying virtualized environments designed to plug into the VDC seamlessly upon arrival are options that should be seriously considered as this will allow the most significant set of communications capabilities to be put into operational use in the shortest period of time.
1.5 Observation / Discussion	**Conclusion / Recommendation**
Being able to "fight tonight" is increasingly becoming a requirement. The standing plans discussed previously in section 1.4 go a long away to making sure the capability exists from a communications perspective to do so.	Defining and consolidating doctrine (procedures) that are executable in a moment's notice is a separate but complimentary effort. As with any doctrine, training, exercising, evaluating, and revising are required to ensure it is and remains relevant and executable.
1.6 Observation / Discussion	**Conclusion / Recommendation**
The capabilities that are required at deployed locations should be defined in detail based on operational requirements. This would include NATO reports and returns.	The goal is for the '6' organization to have a clear understanding of what the Commander, Joint Operations Center (JOC) Director, Battle Staff, etc. needs to execute. This would include capabilities required by all portions of the staff to include administrative, logistics, intelligence, operations, planning, information exchange, training, morale, and more. The '6' organization should design the technical implementation to execute. If done correctly, a staff should be able to show up and be able to execute all tasks that were predefined in garrison.

ITEM 2: ORGANIZATION

2.1 Observation / Discussion	Conclusion / Recommendation
It is important to ensure that the full scope of responsibilities and requirements for each organization is fully defined. This should be accomplished through formal orders, and supplemented using other forms of communications such as meetings and e-mails.	More details are better than few when defining organizational responsibilities. Broad requests for support using terms like “assist” leave too much open to interpretation and increases the likelihood a support entity will misunderstand the full scope of their responsibilities, to include specifics such as number and type of personnel to bring, training and technical expertise requirements of personnel, equipment requirements, task organization, battle rhythm, and more. Specified tasks are a necessity that eliminates confusion and facilitates constructive feedback. Component Commands, after receiving operational level orders, should develop their own orders for their component and attached units with even more specified details. This not only continues to mature planning at all levels, but also provides confirmation to the operational headquarters that their intent and scheme of maneuver is understood and being planned for execution in a manner that is expected. Setting specific goals and milestones and assigning responsibilities for them is a useful tactic as well. This makes clear the expected timeline for how operational capability will mature as it reaches Initial Operational Capability (IOC) and Full Operational Capability (FOC). Opportunities should be sought out to simulate how day to day operations will be conducted during each phase of the operation, which will facilitate a further understanding of reports and communications requirements.

ITEM 3: TRAINING	
3.1 Observation / Discussion	**Conclusion / Recommendation**
There is a significant training opportunity that exists in building the MPE instantiation. Unfortunately, there is a limited training audience that gets targeted at major exercises like SFCT alone.	Periodically building these instantiations in garrison is a way to provide this training capability at low (relative) cost. Later in this report, the value in this from an operational capability verification will be discussed, but the training value is import to consider as well. While this network is being built, and key personnel are being trained, there is additional opportunity to conduct other maintenance functions, such as patching software, which also is a worthwhile training experience.
3.2 Observation / Discussion	**Conclusion / Recommendation**
Using a fully virtualized infrastructure provides for significant value, especially for increased training.	Training will be able to be conducted on various aspects of the mission network to include setup, testing, interoperability, patching, vulnerability management, and configuration management. While this can be done on physical infrastructure, the ability to conduct training and then delete the virtual infrastructure created allows for concurrent realism with no impact to operational networks, a much wider array of topics that can be taught, and any number of simulated scenarios that can be presented.
3.3 Observation / Discussion	**Conclusion / Recommendation**
The FMN construct is complicated, spanning multiple documents that are of significant size in both breadth and depth. While this ensures that details are covered thoroughly and that nations can fully understand and execute using the documents, it does make fully understanding unlikely unless one is heavily involved in a full time role.	In order to mitigate this challenge, more strategic messaging is required. FMN is misunderstood and misconceptions can be mitigated with a comprehensive set of articles, briefs, etc. Training modules that cover the FMN framework should also be developed. These should be broken down into manageable portions that are targeted to specific audiences, to include senior leadership, so that personnel from the various nations can have a more complete understanding of FMN and the role the construct plays in ensuring nations can

	properly interoperate in accordance with the framework. This would significantly increase the knowledge of FMN, which is important for communications personnel, but also important for all personnel as they plan to operate with partner nations.

ITEM 4: MATERIEL

4.1 Observation / Discussion	Conclusion / Recommendation
A large physical footprint for network infrastructure is not conducive for mission networks. Expanded infrastructure also increases heat generation, HVAC requirements, fuel requirements, transportation/logistics complications, vulnerabilities to threats, personnel required, etc.	It is necessary to reduce the network footprint of mission networks that are on site. The smaller and more mobile they are, the less of an impact the aforementioned issues will be. The modularity of the mission network will be of utmost importance in order to achieve COOP capabilities. Given that headquarters locations will be subject to various threats, being able to move locations in short order will likely be a requirement, and one that is hard to accomplish with significant infrastructure in place that is limited in its mobility.

4.2 Observation / Discussion	Conclusion / Recommendation
NATO/NATO Communication and Information Agency (NCIA) developed functional services are not used consistently.	Using functional services that are developed by NATO/NCIA is not required, but has both positive and negative aspects that should be examined. On the positive side, using these software sets or systems provide for a much clearer set of configuration instructions required to make the same software interoperable between nations. Additionally, the infrastructure required does not necessarily reside with one nation or organization for all functional services. This allows the services to be provided from multiple points, reducing single points of failures and reducing individual national contributions. Interoperability ease increases as well in this situation, meaning that configurations are less complex and setup time is also reduced. Alternatively, using these systems and/or software shifts funding for development to NATO/NCIA, which is not always desirable from a national perspective. Additionally, use of this software requires software licenses to be purchased in order to use the software, which can be costly. Interoperability with other national systems and software is also not guaranteed with technical solutions (cross-domain, middleware, etc.) required to be implemented to transfer data from one national system to another. Training on non-national systems would be required, as would funding

	for any training that requires travel to complete. So, the impact of shifting to use a NATO/NCIA system or software should be carefully analyzed, with all variables taken into account. What should be avoided is not using the NATO/NCIA system when there is not an equivalent national system. This could result in information sharing gaps where some nations are sharing data, but others are not, which increases operational risk.
4.3 Observation / Discussion	**Conclusion / Recommendation**
Using thick clients (laptops) as end-user workstations adds significant security risks in terms of insider threats, configuration management, vulnerability management, and classified material control.	Shifting to Virtual Desktop Infrastructure (VDI), to include thin clients, will significantly reduce these risks. Configuration is common between most end-user sessions, and those that are not are able to be more easily customized. Because of the lack of ports and drives available, the risk of data exfiltration by an insider is significantly reduced, although this does have an information exchange drawback that could complicate fairly common Universal Serial Bus (USB) Thumb Drive or Compact Disc (CD) transfers between nations, so a valid and secure means of information exchange between nations may need additional investment. Because all of the end-user stations would not have their own configurations, vulnerability management becomes significantly simplified. A computer that cannot or has not received recent patches no longer becomes an easy avenue of approach for a determined adversary. Lastly, with data not being stored locally, but only on the server or other associated server/cloud infrastructure, the likelihood of misplacing or mishandling classified data is reduced.
4.4 Observation / Discussion	**Conclusion / Recommendation**
Network management tools in use (What's Up Gold primarily) is an acceptable tool to have available, especially for level one technicians, but is not comprehensive enough to provide a real-time situational awareness picture to leadership, either locally or remote.	Additional and improved network management tools are needed. Tools in use primarily give information about up/down status, but little extra amplifying information is available without significant extra configuration. Network management tools should be able to show information related to network and

	system performance to include utilization, response time, and throughput. These tools should also have configuration management (including network discovery) and fault management functions. Ideally, these tools would be built in a framework that leverages Information Technology Infrastructure Library (ITIL) best practices, especially a help desk functionality, ticketing system, as well as incident, problem, configuration, and change management functionality. Network management tools should also have a security component (or accompanying tool) that is able to communicate information regarding status of network defense devices, endpoint protection, access controls, cyber incidents, vulnerability management, and more. At the operational level specifically, it is required to not only be able to examine your own network, but also the networks of those you are connected to, supporting, or supported by. Ultimately, network management tools should be able to display a wide ranging set of data and information through various interfaces that should be available and able to be fine-tuned to respective audiences (including the commander, watch floor, etc.) in multiple locations.
4.5 Observation / Discussion	**Conclusion / Recommendation**
The VDC model, where a shared, virtual computing environment analogous to an enclave in a physical datacenter is available for use, appears to be an effective one and should be duplicated.	Cloud infrastructure is needed for both VDC and private cloud at deployed sites and this model appears to have been effective. As other network instantiations are examined or other entities are looking to improve their IT infrastructure, the primary consideration should be both a data center that can be reached back to remotely, but also a local private cloud infrastructure that is constantly synchronizing with the main data center. This enables operations to continue when units are disconnected from the main data center. The likelihood of this happening on purpose or inadvertently for various periods of time is very high. Planning for any capability is not also available locally, not able to be operated in a disconnected manner for a period of time, and not able to resynchronize upon reconnection adds significant operational risk.

4.6 Observation / Discussion	**Conclusion / Recommendation**
The physical space, material, and services required by the local network instantiation complicates the deployment from multiples points of view, to include how long it takes to set up, how much it weighs, how easy it is to move, how secure it is in transit, how much HVAC is required, how much fuel is required, how many personnel are required, and more.	The tactical processing node, and other similar technologies that virtualize most or all servers and user workstations brings significant capabilities in a small and lightweight package. This type of investment would significantly reduce operational risk and address the risks associated with the current infrastructure deployment, but does come with a significant up front monetary investment, although, large cost savings do occur after initial investment. Capabilities like this should be considered for all mobile command posts and for some special purpose units that are expeditionary in nature. There is also a direct application to afloat naval vessels that are constrained in the physical space available.
4.7 Observation / Discussion	**Conclusion / Recommendation**
There was no use of mobile devices or applications during SFCT. In fact, all mobile devices were banned from the area.	Moving to using mobile devices to compliment VDI is the next step of maturity in delivering information in a relevant and timely manner. One of the points brought up in the DV session was the overwhelming number of applications and the complexity of those applications in use. Another point that was related is that many of the applications in use have a lot of capability, but only 5% of that capability is ever really used by end users. These points argue for a mobile version of the application to provide the vast majority of the information and features required. Using complimentary mobile applications allows for quick delivery of essential information, but without the training requirements that would be needed for full understanding of a complete software application. Other standard positive aspects of mobile applications to include simplified user interface, on the move access, simplified updates, unified communications, etc. all apply. The lack of use of mobility devices and associated applications by most, if not all, personnel is severely reducing the efficiency and effectiveness that could be gained for all operational processes.

4.8 Observation / Discussion	**Conclusion / Recommendation**
The main visual displays in use were not optimal. They were small, not dynamic, relied on projectors (which use high failure rate and expensive bulbs) and were not utilized by personnel.	Moving to a wall of flat screens that are dynamic in nature for the watch floor should be investigated. This would allow different screens to be used for different purposes, or multiple screens to be used for the same purpose. The goal of a watch floor visual display is to enhance the decision making capability of those on the watch floor. If the displays are static, not providing relevant information, and burning up resources (projector bulbs in this case), it is more useful for them to be off, which is not the desired end state. There should be a Standard Operating Procedure (SOP) for what is on what screen at all times so that when the Commander or Director is on the watch floor, they know exactly where to look for information they need. Of course, when operations or evolutions dictate, the screen displays should be adjusted to provide the most relevant and timely information to those that are using it.
4.9 Observation / Discussion	**Conclusion / Recommendation**
The SharePoint design and configuration was done on the fly on site. This slowed down communications between partnering nations and took significant time. Using SharePoint as a live, dynamic information sharing tool was not demonstrated, although basic functionality and configuration was.	SharePoint portals should be built in advance to include complete structures. Population of data on these portals should be done in advance as much as possible. Of course, if a mission network instantiation is just stood up, this could take time, and may have to wait until on site, but at least a standardized template can be used to save time and facilitate information management process repeatability. Preferably, the mission network to include SharePoint would be set up well in advance. Additionally, determinations should be made in advance regarding trust structures that would enable access from mission partners. Training will have to be conducted on proper control of classified information and where on the portals certain information can or can't be placed. The best training will be daily use of the same policies and procedures in garrison as would be used in the field. Lastly, as configuration of SharePoint portals is a moderately challenging endeavor, detailed procedures should be

	developed that will enable expedited setup, and SharePoint training should be purchased for information managers. Establishing avenues for information sharing should be one of the top priorities for early setup, as this is a critical enabler for getting systems properly configured and facilitating early operational capability.

ITEM 5: PERSONNEL	
5.1 Observation / Discussion	**Conclusion / Recommendation**
Dedicated support from civilian personnel, whether they are government employees or contractors, fill a critical capability gap not available in active duty personnel.	Civilian personnel played a significant role in the setup and testing of the SFCT network (Cisco and Microsoft subject matter experts specifically). Without their support, significant challenges would have presented themselves. These personnel represent a significant resource that should be included into future plans for network setup and support for future exercises and operations. While the desire to have active duty personnel be able to fill these roles is understandable, unfortunately, it would be extremely difficult to find personnel that would have the technical breadth and depth that is required and this is more easily found in the civilian sector.

ITEM 6: INTEROPERABILITY

6.1 Observation / Discussion	**Conclusion / Recommendation**
Flexibility with joining of unplanned units, or unanticipated partners was not demonstrated.	Flexibility of a mission network is key. Standing plans should be established that will have documented procedures for likely eventualities. This would include whether a new unit is arriving in the area, a unit moves, you need to share information with a civilian partner, you have a new data source, etc. This planning is challenging for communications personnel to accomplish alone. Partnering with operations, intelligence, and logistics personnel is essential for developing these type of requirements so that appropriate procedures and configurations can be developed, documented, tested, and put into practice.
6.2 Observation / Discussion	**Conclusion / Recommendation**
A robust change management process was not observed, which could cause significant variance in configurations and severely impact mission effectiveness.	Trust in configurations and testing is essential. Configurations must be validated to confirm they are correct and established as a configuration baseline. Once configurations are implemented, verification and testing is required. As issues are identified, all parties can make test changes to configurations and if successful, can propose that as permanent configuration changes that would be implemented into technical documentation as part of the change management process and result in a new configuration baseline. Not implementing networks in accordance with the established configuration baseline and not having a change management process, especially with the number of units and systems that are attempting to be interconnected, is likely to slow down the achievement of IOC. Additionally, SFCT, as currently designed, is executed under ideal conditions, with most participating entities on site. This will likely not be the case in an actual operational scenario, so in-person assistance which was taken advantage of at SFCT will not be an available option for troubleshooting. Sharing configuration baselines between nations ahead of time and exercising the federation with systems built in accordance

	with those baselines will significantly speed up the process of federation during SFCT and reduce the amount of configuration changes that are needed on site at SFCT.
6.3 Observation / Discussion	**Conclusion / Recommendation**
The status of information sharing systems and processes was not always clear. The situational awareness tool in use (What's Up Gold) did not always have the status correct, showing an "up" connection while users were having problems.	It is important to maintain situational awareness of the status of information sharing between partners. Sometimes, an up-down status may be deceiving, with higher layers presenting issues that affects interoperability, while lower layers show no apparent issues. If that data is being used regularly in real time (like live chat or a data stream), this issue would be recognized in short order. But, if that information is not being used as often, it could only be realized at the exact moment when it is needed, which is too late. So, periodic validation of information sharing capabilities will be required.
6.4 Observation / Discussion	**Conclusion / Recommendation**
SFCT presented a good opportunity to implement a mission network instantiation, but it would be more effective if most of the work was done in advance.	All efforts to design, build, test, authorize, federate, operate, etc. a MPE instantiation should be accomplished in garrison as much as possible. Participation in smaller, more frequent interoperability validation events should be investigated. This would allow for a significant opportunity to conduct interoperability testing prior to a major event like SFCT, as well as maintain a steady-state level of readiness for interoperable networks. Additionally, SFCT is an exercise focused on testing and confirmation, not experimentation. While there is not room in the current SFCT format for experimentation, Coalition Warrior Interoperability eXercise (CWIX) should be leveraged to include experiments and concepts that could be tested and matured in time for use during the follow-on iterations of SFCT.

6.5 Observation / Discussion	Conclusion / Recommendation
All nations need some way to define their current capability with respect to interoperability with partners and define a way ahead for improving that capability.	Development of an interoperability maturity model should be investigated. This should focus on the maturity as it progresses from technical, then procedural, then operational. As an additional perspective, this could be broken down by capability, then system, then component. This analysis should be done to evaluate the as-is situation, and various to-be situations that are spread out over a timeline representing growth in maturity of interoperability capability. This analysis would inform discussions and decisions on strategy, acquisitions, exercises, initiatives, and other key decisions. The goal would be to improve across the maturity model as time progresses. For exercises, a desired maturity should be demonstrated, with new capabilities and systems being implemented in a testing manner to allow for potential growth or validation of growth for application to the long term model. There is an option for a third dimension of the model, which would depict the level of operational effort, or the size of an operation, as not all operations are the same and as such do not require the same level of operational capabilities to be fielded. This perspective is especially useful for operational commanders, as they would have a much clearer understanding of actual capabilities their units have with respect to interoperability, a key addition to periodic readiness assessments and understandings that must be in place.

ITEM 7: EXECUTION

7.1 Observation / Discussion	**Conclusion / Recommendation**
Engineering of the MPE at the SFCT exercise site is a distinct effort that requires the right expertise. Clarity in the requirements is essential to ensure success.	It is important to delineate exactly what units will be tasked with providing what expertise and equipment and what specific responsibilities and tasks they will be assigned. Given this information, subordinate or partnering units will be able to conduct proper preparations. Assumptions regarding tasks should be kept to a minimum, a result of effective planning. This preparation will allow units assigned with network engineering responsibilities to fully understand the scope of their responsibilities and subsequently devise a plan for execution, which may include requirements for additional expertise, equipment, training, procurement, and support. A complete understanding of the requirements, especially if they are out of scope for a normal request, should be defined in detail up front so that appropriate Memorandums Of Understanding (MOU) and Service Level Agreements (SLA) can be developed and put into place.
7.2 Observation / Discussion	**Conclusion / Recommendation**
Much of the establishment of the MPE happened on site at SFCT. While it worked for this exercise, it is not an effective or efficient way of executing the MPE and would cause considerable challenges if it had to be implemented in an operational environment.	Building as much of the MPE as possible before arriving at SFCT, similar exercises, or actual operations is essential. First, this makes it much easier on units that are engineering the MPE solution to ensure they have the right material and expertise to build what is being requested. This also allows for configuration changes that would normally require engineering level support to be sought, something that is much more complicated to secure during an exercise or during operations. Additionally, this also allows for tests that will be evaluated during the exercise to be executed. This significantly speeds up the testing and confirmation process, as well as provides the opportunity to identify failed tests earlier, as well as the pursuit of solutions for these identified issues. Also, building the MPE early significantly reduces the time required on

	the exercise site. The costs savings on delaying arrival at the exercise site could be significant, but it must be considered in conjunction with other partner nations and when they need capabilities they are not providing themselves or an operational system to interconnect with. Lastly, the more of the MPE that is built beforehand and utilized, the more likely it is that issues are identified, processes are properly implemented, and operational use cases and integration into the normal operational battle rhythm is validated.
7.3 Observation / Discussion	**Conclusion / Recommendation**
Many of the test cases that were executed at SFCT could have been run in garrison if an MPE instantiation was built and operational then, saving significant amounts of time and money.	As discussed in 7.2, building and having a standing MPE would result in significant efficiencies being gained at exercises like SFCT. One of these is running test cases. Tests that do not require an active partner to be connected could be validated beforehand. This way, only the confirmation of the test would be required on site with minimal requirements for initial configuration or setup being required. This would mean that systems and personnel would not have to be deployed as early. Additionally, if other partners developed a similar level of MPE readiness, then partner to partner tests could also be validated before the exercise as well.
7.4 Observation / Discussion	**Conclusion / Recommendation**
Although SFCT is a communications exercise, communications capabilities are established in order to enable operations, intelligence, logistics, administrative, and other personnel to conduct various missions and tasks. So, while communications pathways were tested and validated during SFCT, the operational piece was not tested or exercised.	While full operational capability is tested in future TRIDENT exercises, without some operational testing or process validation, there runs an increased risk that success identified during SFCT will not translate to operational success in future exercises or combat operations. Operational test cases should be implemented and exercised during the last 2-3 days of SFCT. This will allow operational personnel to descend on a mature and tested communications capability and validate that daily processes of non-communications personnel can be executed. This should start with execution of the daily unit battle rhythm and standard meetings, but should progress to more realistic combat/operational

	scenarios such as communicating with forces (air, maritime, and land), tracking operations in real time, establishing and utilizing data feeds from live operational systems (unmanned, remote camera/sensing, cooperative engagement, etc.). Ultimately, what should be avoided is a non-communicator having to use the MPE that is built, but that MPE missing key capabilities needed to conduct daily or combat operations. A liaison that is an operations center director or battle watch captain that is a full-time participant in the exercise would be useful to make sure that any gaps that do exist are identified early, corrected if possible, and if not, planned for future exercise iterations. Any capabilities that are not currently available should be identified as risks, with mitigations put into place to ensure no capability gaps exist or that they are minimized. The deploying team of non-communicators that will eventually use the MPE to conduct exercises and operations should know exactly what capabilities they will have at their disposal and which they will not so they can put into place their own mitigations such as continued external support from garrison.
7.5 Observation / Discussion	**Conclusion / Recommendation**
SFCT was executed as a static exercise, meaning no movement of gear, facilities, or personnel took place except for deployment and redeployment. This only allows for one iteration of execution of the setup and take-down process.	During actual operations, it is unlikely that a capability set of this magnitude will be able to stay stationary given the various threats and associated risks that a stationary facility would face. So, the process of setup and take-down of the various systems and equipment should be exercised. This is something that could be done before the exercise. Additionally, in order to be successful, stand up and take-down speed is of the essence and needs to be exercised and tested. There will be times when quick, limited setup might also be required. This should also be exercised and tested. Many of these types of evolutions could be done as mini-exercises in garrison to refine skills and techniques.

7.6 Observation / Discussion	Conclusion / Recommendation
Organization and execution of test assignment, execution, tracking, and reporting was developed on-site, during the exercise, which did not allow for preparation for testing, or reporting on testing results. It also contributed to confusion regarding daily testing requirements and goals, as well as an accurate understanding of testing progress.	To accomplish the most gain from the testing and confirmation process, planning and execution should begin much earlier than the exercise. A comprehensive test plan should be designed before executing an exercise that focuses on testing for FMN confirmation. This plan should cover all aspects of the testing process to including assignment, execution, tracking, and reporting. All personnel, to include a test director, testing team leads, and testing teams should be identified. The test director should be defined early enough to allow the opportunity to attend the TCC and develop an overall test execution plan for the exercise. Additionally, the test director should be able to use this opportunity to organize the testing teams, coordinate with civilian expertise, and prioritize efforts that would allow for as much pre-testing to be done as possible before deployment. To facilitate this, configuration and testing documents should be shared widely in draft form before the TCC and finalized soon after. Leaders of each of the testing areas should also be identified early to facilitate communication and planning before the exercise. Testing teams should be fully identified before the exercise and given information to properly prepare. Delaying putting together testing teams until arrival or the start of the exercise will prove to be much too late. During preparation, determining how communications should be executed between the testing teams and the test cell liaison should be identified. These teams are in separate locations, so using chat may be an option, but it also may be just as efficient to coordinate test status face-to face (if possible). A testing battle rhythm should be developed that ensures participation in all appropriate testing meetings and attendance at all test presentations. Personnel should also understand who the test leads are who are responsible for testing of systems or interfaces that are shared between nations and set up opportunities to collaborate as the interfaces are configured on both sides. This will help develop the mutual relationship and trust needed that will ease future collaboration and troubleshooting efforts. Testing progress should be closely tracked and displayed, allowing for easier

	understanding of progress, and shared with higher headquarters (HHQ) in a real-time basis. While the real-time progress really isn't necessary for testing results, it does test the capability to distribute information to HHQ, a capability that will be needed in both exercise and operational scenarios. Close tracking of testing requirements will also eliminates confusion from test teams and allows the test director to prioritize efforts on tests (or associated configurations) that aren't going well or on tests that are behind schedule. This also allows the test director to understand when outside assistance is needed and communicate that requirement at an appropriate testing meeting. The testing plan should be laid out so that tests are conducted in the appropriate order. Tests should not be spread out evenly over the exercise, but should be front loaded so that tests that have the potential to cause challenges are quickly identified. This allows for quicker resolution, which is important especially when testing systems other nations are depending on. Lastly, reporting regarding testing progress should be done in a standardized and pre-organized manner. Not only should this information cover what tests were accomplished that day, but it should also identify challenges with specific tests, opportunities to speed up specific tests, and progress comparison to the original test plan and schedule.
7.7 Observation / Discussion	**Conclusion / Recommendation**
The realism provided by the SFCT exercise provides important value. There will be an effort, especially as interoperability improves, to conduct testing and validation in garrison, which has value, but is not a substitute for execution at SFCT.	Rising confidence in the ability to conduct testing and validation in garrison will have the effect of causing additional consideration of whether the cost in equipment, manpower, time, and money is worth it to deploy for such an extensive long-term exercise. Continued participation should be encouraged as there really is no substitute for actually deploying communication and networking capabilities and making sure they work in an operational scenario. Additionally, partnerships, relationships with partner nations, and the trust and confidence that come with that, are not able to be cultivated while in garrison. Lastly, exercising the logistic piece of the exercise, including developing

	agreements with partner and host nations, is something that is hard to substitute without onsite attendance.
7.8 Observation / Discussion	**Conclusion / Recommendation**
The NATO Cyber Defense Cell was stood up at the SFCT 17 exercise and is anticipated for future exercises. Leveraging this team is an opportunity that should be taken advantage of.	Network vulnerability assessments and penetration testing should be conducted from both inside the mission enclave boundary as well as from outside the boundary, which coordinating with the NATO Cyber Defense Cell allows, but can also be done by national means. It is important to ensure that lateral movement within the network by exercise participants is properly prevented. This is a prudent practice that also prevents the possibility of partner nation's systems being used as a pivot point for an actor with malicious intent. It is important to realize that the use of a mission network for operations provides the ability to move critical operational information from classified national systems to a network instantiation custom built for that operation. While this provides significant value, it also increases the likelihood that the mission network will be a target of adversary attack. Therefore, protection and defense of the network should be of utmost importance. Of course, this mission network is also one that needs to operate with mission partners. A detailed risk analysis and risk mitigation implementation needs to be introduced and executed that balances these requirements of security and interoperability.
7.9 Observation / Discussion	**Conclusion / Recommendation**
Deployment timelines should be appropriately defined to ensure a leadership cell is on the ground as support units are arriving.	A leadership presence on site from the first day ensures that intent is immediately available to support units, clarifications are able to be sought, and prevents rework from having to be accomplished. This leadership cell should be primarily responsible for coordinating with other nations and the exercise leadership to make sure that national contributions are in line with other nations and exercise leadership expectations.

7.10 Observation / Discussion	Conclusion / Recommendation
Upon completion of the SFCT exercise it is important to save all configurations, settings, and other technical details required to stand up the MPE in support of future exercises or actual operations.	Configuration details and appropriate configuration control after an exercise ensures that lessons identified during the exercise are actually learned and that future exercises and operations are appropriately leveraging a known good end state and progressing from there. It is equally important to not keep these configurations residing in a single place, or without being tested periodically in between exercises. It is unknown what unit will provide core services in the future. So, configurations, guides, tactics, techniques, procedures (TTP), and any other details needed to ensure another unit could stand up a duplicate capability needs to be centrally housed and shared with those that may need it. Of course, having configurations on hand is only a portion of what will be needed to fully stand up an MPE instantiation. So, this capability should be exercised at units periodically, at least twice per year, per potential communications support unit, to ensure that the MPE for any given situation could be set up quickly. Lessons learned from each one of these evolutions, per unit, should be collected, consolidated, and result in documentation changes (controlled by a standing configuration control board) that are used during follow-on iterations. The goal is a seamless stand-up of an MPE instantiation in the shortest time possible to provide an operational commander the capabilities they need to conduct operations, and periodic exercises will go a long way to reducing the risks associated with this endeavor.
7.11 Observation / Discussion	**Conclusion / Recommendation**
Testing of the SFCT did not simulate the full amount of bandwidth that would be required and utilized by the systems and personnel in an actual operational scenario.	Bandwidth available to a forward deployed headquarters is a limited resource that will be used up very quickly in an operational scenario. During SFCT, a comprehensive test should be done to ensure that the various systems under full operational load will not be utilizing more bandwidth than what is available. Other considerations should include whether and how much of the mission

	network is available for morale and welfare use, or if a separate network will be required for this purpose that will have its own bandwidth requirements. Network maneuver will also need to be tested, so that, as required, operational necessities like video teleconference or a live feed could be prioritized, restrictions could be put into place to optimize bandwidth or to establish specific operational security limitations, or network routes could be adjusted. Additionally, bandwidth available may vary depending on the resources that are available. In a communications degraded or denied environment, or a situation where significant amounts of bandwidth are not available, capabilities and system use will have to be appropriately prioritized to ensure that the most urgent or important operational requirements are met. This is a risk management discussion that must take place before exercises and operations by operational personnel and codified into configuration management policy that will have to be adjusted as conditions and the associated bandwidth available changes. Lastly, it should be assumed that an MPE instantiation should be able to fully federate and operate on satellite communications alone. Future iterations of SFCT should incorporate this to determine how setup and federation would have to change if the bandwidth capacity was limited.

ITEM 8: FUTURE CONCEPTS

8.1 Observation / Discussion	Conclusion / Recommendation
Actual capabilities and gaps associated with a forward headquarters should be identified, as should a desired future state.	The capabilities and gaps of a forward headquarters should be defined, along with future iterations that grow capabilities and eliminate gaps. So, for example, if a commander feels like they need unmanned system feeds, needs to control unmanned systems, wants to be able to show operations (like special operations) in real time, needs to display network vulnerabilities or network operations, see live camera view, see live logistics status', etc. that should all be defined. This enables the commander to develop a maturity model that is useful for planning, prioritizing, and budgeting future growth. This will grow the maturity of the capabilities of the headquarters over time, allow for appropriate investment, and make exercises more relevant and operations more effective.
8.2 Observation / Discussion	**Conclusion / Recommendation**
A forward operational headquarters is a complex system of interactions between the main entity, supporting, supported, and coordinating entities, systems, processes, technologies, relationships, and more. It is a complex system that needs to be better understood in order to make dramatic future improvements.	The complex system that makes up the pieces of an operational headquarters should be modelled and simulated. All interactions, processes, technologies, etc., both internal and external, should be identified, captured, and coded into a model that accurately represents the current state. Goals for a future state should be defined and potential capability improvements should be modeled and included in simulations to determine actual value and impact they would provide. Capabilities that show significant capability increase should be further examined to determine if they are available for potential purchase or if more research is required. Potential improvements to existing systems is also something that could be identified, allowing for significant detail to be added to requirements updates for those systems. Also, personnel make-up and breakdown is something that can be examined, which will allow for a more accurate understanding of the specific knowledge, skills, and abilities that are

	needed in the headquarters. Processes that are effectively modelled can also give insight into the incoming information flows required to make that process effective and outgoing information flows required to inform other processes, to include the commander's situational awareness. Incorporating modelling and simulation into process improvement is a challenging endeavor, but provides an opportunity to design the right operational solution in a model before investing significant time and resources.

ANALYSIS REQUIREMENT TEMPLATE

IDENTIFICATION: NATO C2COE 2.7
TITLE: EXERCISE STEADFAST COBALT 2017
CUSTOMER: Unites States European Command (USEUCOM)
CUSTOMER POC: Mr. Robert Watson, ECJ6, robert.l.watson42.civ@mail.mil
STAKEHOLDERS: USEUCOM, USEUCOM service components, and other combatant commanders utilizing a mission partner environment. NATO Command Structure (NCS): Allied Command Operations (ACO), Allied Command Transformation (ACT), NATO Communication and Information Systems Group (NCISG), Joint Warfare Centre (JWC) and Joint Analysis and Lessons Learned Centre (JALLC). NATO Communications and Information Agency (NCIA). NATO Force Structure (NFS): NATO Rapid Deployment Corps Italy (NRDC-ITA), Rapid Reaction Corps France (RRC-FRA), Multinational Corps Northeast (MNC-NE) and other NFS headquarters (HQ) that will federate with mission partners in accordance with the Federated Mission Networking framework.
BACKGROUND / AREA OF OBSERVATION: The United States has participated in STEADFAST COBALT in previous years, but 2017 is the first year that the U.S. would attempt confirmation in accordance with Federated Mission Networking framework Spiral 1.1 specifications. The NATO C2COE embedded with the USEUCOM forward HQ element to observe, provide analysis and feedback, as well as provide best practices for future reference.
ITEMS FOR ANALYSIS: • C2 processes and systems • Configuration management • Operational requirements • Organizational responsibilities • Process improvement • Capability refinement • Risk management • Situational awareness • Operational planning • Future concepts
ANALYSIS DELIVERABLE: This report is the final product of the STEADFAST COBALT 2017 exercise participation by the NATO C2COE.
FORMULATED JOINT ANALYSIS REQUIREMENT: Analyze the C2 exercise element of EXERCISE STEADFAST COBALT 17 which is the Communications Exercise (COMEX) for TRIDENT JUNCTURE (TRJE) and provide recommendations for improvement to make it a more effective and operationally relevant exercise.
TIMELINE: The deadline for this report is Fall 2017.
IMPACT STATEMENT: The purposes of this report is to provide feedback to USEUCOM, as well as provide comprehensive lessons learned for the NCS and NFS, while demonstrating what kind of analysis the NATO C2COE may deliver for its community of interest.

REFERENCES

A. U.S. Department of Defense Instruction 8110.01 - Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD; 25 November 2014

B. USEUCOM TASKORD – SUPPORT TO NATO EXERCISE STEADFAST COBALT

C. Evaluation Criteria for STEADFAST COBALT 2017

D. NATO Functional Services Diagrams for STEADFAST COBALT 2017 / NRF 2018

E. Kucukaksoy, I. (2016, July). NATO capability development and interoperability. The Three Swords Magazine. Retrieved from http://www.jwc.nato.int/images/stories/_news_items_/2016/LT_GEN_Lofgren_interview.pdf

ABBREVIATIONS

ACO	Allied Command Operations
ACT	Allied Command Transformation
ATO	Authority to Operate
C2	Command and Control
C2COE	Command and Control Centre of Excellence
CD	Compact Disc
CIAV	Coalition Interoperability Assessment Validation
COMEX	Communications Exercise
COOP	Continuity of Operations
DOD	United States Department of Defense
DOTMLPFI	Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability
DV	Distinguished Visitor
FOC	Full Operational Capability
FMN	Federated Mission Networking
FRA	France
HHQ	Higher Headquarters
HQ	Headquarters
HVAC	Heating, Ventilation, and Air Conditioning
IOC	Initial Operational Capability
IP	Internet Protocol
ITA	Italy
ITIL	Information Technology Infrastrucuture Library
JALLC	Joint Analysis and Lessons Learned Centre
JCSE	Joint Communication Support Element
JMEI	Joining, Membership, and Exit Instructions
JOC	Joint Operations Center
JTIMS	Joint Training Information Management System
JWC	Joint Warfare Center
MNC-NE	Multinational Corps Notheast
MPE	Mission Partner Environment
MOU	Memorandum of Understanding
NATO	North Atlantic Treaty Organisation
NCIA	NATO Communication and Information Ageency
NCISG	NATO Communication and Information Systems Group
NCS	NATO Command Structure
NFS	NATO Force Structure
NLD	Netherlands
NRDC	NATO Rapid Deployable Corps
NRF	NATO Response Force
OPCON	Operational Control
RRC	Rapid Reaction Corps
SFCT	STEADFAST COBALT
SHAPE	Supreme Headquarters Allied Powers Europe
SLA	Service Level Argeement
SOP	Standard Operating Procedure
TASKORD	Tasking Order
TCC	Technical Coordination Conference
TRJE	Trident Juncture
TTP	Tactics, Techniques, and Procedures
US	United States
USA	United States of America
USB	Universal Serial Bus
USEUCOM	United States European Command
USTRANSCOM	United States Transportation Command
VDC	Virtual Data Center
VDI	Virtual desktop Infrastructure
WAN	Wide Area Network