24th ICCRTS

"Managing Cyber Risk to Mission"

Aligning Command and Control (C2) and Cyber Risk to Mission

Topic 1: Cyber Risk to Mission

Mr. Ken D. Teske

Mr. Ken D. Teske (Key Management Solutions)

Mr. Mark Miller (Key Management Solutions)

Mr. Patrick Guerin (Key Management Solutions)

Point of Contact

Ken D. Teske

Key Management Solutions

223 N Wahsatch Ave, STE 206

Colorado Springs, Colorado 80903-2253

(757) 510-0915 kteske@kmssecurity.com

Abstract

Mission Partners, Coalition Command and Control (C2), and Cyber forces must develop options and capabilities that enhance inter-dependence and further their alignment "harmonization" to increase everyone's effectiveness and understanding, while reducing the Cyber risk to the mission. The following four principles are a necessity in order to achieve alignment and integration: Common view with goals and objectives; Common understanding of capabilities; Alignment of efforts to ensure coherency; and Assessment to change course or direction as needed.

Both alignment and integration will help address the challenges associated with any Cyber Risk to Mission in today's ever-changing environment. Applying and evolving a framework approach that was discussed in the 19th ICCRTS, paper (003), 21st ICCRTS, paper (001), and 22nd ICCRTS, paper (004) demonstrates the importance of comprehending that each and every partner; Special Operations, Conventional Forces, Ministries, Departments, Bureaus, and Agencies are important to better understand and confront C2 and Cyber risk problems and issues.

We must use our collective lessons learned, best practices, approaches, and strategies identifying common goals, areas of interest, capabilities, and common categories of effort to be applied by each of the organizations as the focus area to maximize our Cyber-enabled capabilities.

Introduction

In September of 2011 Admiral McRaven the USSOCOM Commander said "one of the explicit lessons of the last decade of conflict is the absolute necessity to share information, plan, and operate in concert with our interagency and foreign partners" [Ref. M]. This document continues to describe the multi-year evolution of a Command and Control (C2) project enabling the Alignment, Synchronization, and Integration framework and methodology that will be traced through a set of illustrative use cases. A Methodology to Improving Unity of Effort for Mission Partner Planning, paper (003) was first discussed in the 19th International Command and Control Research and Technology Symposium (ICCRTS) [Ref. A, N, T]. We have explored and continue to explore methods and approaches developed by others to ensure that leaders are able to access and incorporate the best tools to address and align their complex endeavors.

The NATO Research and Technology Organization Studies Analysis and Simulation panel 065 characterizes complex endeavors as; Such endeavors are "distinguished by one or more of the following characteristics: First, the number and diversity of participants is such that there are multiple interdependent chains of command, the intents and priorities of the participants conflict with one another or their components have significantly different weights, or the participants' perceptions of the situation differ in important ways. Second, the effects space spans multiple domains and there is a lack of understanding of networked cause and effect relationships, a resulting inability to accurately predict all of the relevant effects that are likely to arrive from alternative courses of action, and therefore, a lack of ability to appropriately react to undesirable effects by making timely decisions, developing appropriate plans, and taking the necessary actions" [Ref. Q]. The current NATO Research and Technology Organization Studies Analysis and Simulation panel 143 is looking at the cyber impacts for ongoing complex endeavors as well.

To understand why this framework has evolved, we must look at a theme that continues to resurface from operational focused leaders at many levels across the world. The statements always sound something like, if our cyber warriors work together, then we will be able to address our C2 and cyber challenges. There is no end to the higher-level philosophy, guidance and directions to work in this manner with C2 and cyber partners through the North Atlantic Treaty Organization (NATO), Defense Departments, others agencies and organizations. “Through the NATO Defence Planning Process (NDPP), NATO identifies capabilities and promotes their development and acquisition by Allies so that it can meet its [cyber] security and defence objectives. By participating voluntarily in the NDPP, Allies can harmonise their national [cyber] defence plans with those of NATO” [Ref. H].

In order to accomplish Alignment, Synchronization, and Integration, all C2 and cyber partners must act together with a “common” starting point to begin the process and ensure shared understanding of the lexicons, capabilities, limitations, and consequences to C2 and cyber. In the National Security Strategy of 2015, President Obama specifies that to succeed “we will lead with capable partners, mobilizing collective action and building partner capacity to address global challenges” [Ref. L]. In an ideal world, organizations worldwide concerned with key issues would operate from an overarching collective strategic cyber plan at the global, regional and country-level to ensure alignment of various efforts. The fact of the matter is that everyone faces significant complications to ensure that that their plans are based on collective assessments of conditions and appropriately aligned to develop, produce, and maintain a common viewpoint.

Background

“In the summer of 2010, United States Northern Command originally proposed to United States Joint Forces Command concepts division a synchronization model to help improve

interagency communication and unity of effort in steady state planning. That model initially evolved into the Planning Synchronization Framework and, in partnership with United States Southern Command, United States Special Operations Command and others, became the foundation for the framework methodology today" [Ref. A]. Chairman of the Joint Chiefs of Staff General Dunford stated that "problem sets are trans-regional, multi-domain, defy legacy phasing, and require global integration…we must design our future Joint Force and Command and Control to best respond to this new paradigm…considering all our actions will have global implications" [Ref. U]. Commands world-wide need a consistent and institutionalized approach to plan and resource military support for other Agencies toward meeting national and strategic objectives at the execution, operational and campaign levels.

In the National Security Strategy of 2010, President Obama specifies that to succeed we must take a "whole of government approach" that is "deliberate and inclusive of the interagency process, so that we achieve integration of our efforts to implement and monitor operations, policies, and strategies." [Ref. F]. To achieve this all government organizations concerned with national C2 and cyber security should operate from an overarching common plan at the global, regional and national levels to ensure alignment of numerous efforts. This would further be aligned with other governments who are experiencing the same types of hurdles to ensuring their plans are also based on shared assessments of conditions. In order to gain alignment of efforts we must apply these four principles: Common understanding of the situation; Common vision, goals and objectives for the mission; Coordination of efforts to ensure continued coherency; and Common measures of progress and ability to change course as needed.

We continue to observer that within each organization there are differences in priorities that result in critical differences at the Government level that effect all planning. These differences

continue to fall into inhibitors to alignment. The Mission Command White Paper states that "operations will move at the speed of trust." "Trust is the sinew that binds the distributed Joint Force 2020 together, enabling the many to act as one…" [Ref. I]. We will discuss these in greater depth later in this paper.

In their book Power to the Edge, Albert and Hayes (2003) talk about key dimensions of agility that are represented by the synergistic combination of the six following attributes: robustness, resilience, responsiveness, flexibility, innovation and adaptation: [Ref. D]

- Responsiveness: "The ability to react to a change in the environment in a timely manner"
- Robustness: "The ability to maintain effectiveness across a range of tasks, situations, and conditions"
- Flexibility: "The ability to employ multiple ways to succeed and the capacity to move seamlessly between them"
- Resilience: "The ability to react to a change in the environment in a timely manner."
- Innovativeness: "The ability to do new things and the ability to do old things in new ways"
- Adaptiveness: "The ability to change work processes and the ability to change the organization"

We proposed repeatable processes at the 19th ICCRTS in paper (003) titled "A Methodology to Improving Unity of Effort for Mission Partner Planning" research that may be a solution to improve Unity of Effort [Ref. A]. Repeatable in this context refers to the processes, procedures, workflows, and templates that are reusable framework components. Repeatable processes allow a team to make efficient use of framework mechanisms that have proved to be successful in the past and reduce unnecessary variations that can take up time, effort and resources.

We continue to observe that over the last twenty years leaders at all levels have struggled with the requirement to share C2 and cyber security responsibilities with other nations to help address security challenges that we collectively share dealing with countering terrorist criminal networks, supporting peacekeeping operations, institution development for the maintaining of security, law, and order, or working and fighting alongside others with the intent of providing C2 and cyber solutions to achieve collective goals.

Framework Evolution

Understanding that the framework structure, definitions, templates, and how-to instructions are repeatable and reusable provides for real flexibility in its application. The first version addressed the U.S. Combatant Commands (CCMDs) needed to plan and resource military support for Civilian Agencies and improve synchronization toward meeting national and strategic objectives dealing with Countering Transnational Organized Crime (CTOC). The next five illustrative use cases (Post Mali, Information Technology / Information Systems Portfolio, the two Sudan(s), and Global SOF Directory and Repository) have been in previously referenced ICCRTS papers to provide examples describing actions and content involved in supporting leader's tasks and specific projects.

The Alignment, Synchronization, and Integration Framework (ASIF) evolution continued in order to directly support bridging of an existing capability gap in the ability to develop and maintain shared awareness and understanding with all partner nations of both United States Special Operations Command (USSOCOM) J3-International directorate and North Atlantic Treaty Organization (NATO) Special Operations Forces (SOF) Headquarters (NSHQ). We presented this evolution and demonstrated it in the small group setting at the 21st ICCRTS with our paper (001), Improving Alignment and Unity of Effort with mission partners [Ref. S]. Admiral McRaven the

USSOCOM Commander testified to the 113th Congress Senate Armed Services Committee that "USSOCOM is enhancing its global network of SOF to support our interagency and international partners in order to gain expanded situational awareness of emerging threats and opportunities" [Ref. K]. Two additional projects with supporting papers were presented in the 22nd ICCRTS, paper 005 Improving Cyber Security Alignment and Integration and paper 025 Protecting Information Sharing Systems with Commercial Solutions for Classified Encryption that discussed adaptations of the framework methodology and utility. The Complete Business Process Handbook states that "such a comprehensive alignment management concept uniquely recognizes that any organization, department, or even program, even if it has its own mission, vision, strategies, and critical success factors, is only one element of a larger delivery and service mechanism. In nearly all cases the success of strategy to execution depends on the ability to operate in alignment and therefore unity with the rest of the organizations with a common stake in the issues" [Ref. R].

Inhibitors

As mentioned earlier, leaders collectively identify many reasons, rationales, and explanations which impede achievement of alignment of effort. We will call these reasons, rationales and explanations - inhibitors. Table 1 below shows the inhibitors identified over time.

Inhibitors	
1. Differing lexicon, taxonomy, or language	7. No established process (everything is ad hoc)
2. No visibility of efforts and activities	8. Lack of planning resources
3. Confused over mixed messages	9. Uncoordinated efforts
4. Competing priorities	10. Conflicts in planning timelines
5. Disparate activities	11. Silos of information (lack of sharing)
6. No forcing function	12. Lack of interoperability

Table 1: Inhibitors

If the inhibitors degrade the ability to achieve alignment, then it would be a logical assumption that the mitigation of as many of those inhibitors would thereby improve alignment

and synchronization of efforts. However, this is not always easy to address. For example, inhibitor #12 “interoperability”, has multiple U.S. Joint Doctrine definitions e.g. “The ability to operate in synergy in the execution of assigned tasks” [Ref. P, N] and “The condition achieved among communications-electronics systems or items of communications-electronics equipment when data, information or services can be exchanged directly and satisfactorily between them and/or their users” [Ref. G]. These thoughts can also be viewed as inhibitor #1 “differing lexicon, taxonomy, or language”. We continue to learn that however the issue is identified we must look to overcome them in order to achieve a common goal. As the framework continued to change, a new inhibitor emerged that no leader wanted to discuss, “ownership” or “who is in charge.” Like many other areas, Cyber issues do not truly have a particular owner, we needed to have leaders align or arrange groups of cyber problems or capabilities in relation to one another to solve the collective issues as well as national and international-level guidance [Ref. B, C, E, O].

Analysis

Through comment and discussion with C2 and Cyber project leaders on the previous applications of the ASIF and methodology used by other projects, it was apparent that “Substantial Improvement” could be gained if there were majority agreement and operational significance of a Common view with goals and objectives, Common understanding of capabilities and lexicons, Alignment of efforts to ensure coherency, and Assessment to change course or direction as needed are results of implementation of a framework methodology. Evaluation metrics would be based on identification of the inhibitors to alignment of efforts described in Table 1.

In order to measure progress pre-event survey data and weighting would be based on a survey of participants collected upon project commencement. The realization criteria would be determined by setting a target response to all survey questions at a score of 3 or better on a scale

of 1 to 5 – a response of 3 or better would mean that there is no negative reaction to the attribute (inconclusive =1 or 2, neutral =3, possibly =4, conclusively =5). Survey questions would address:

- Usability
- Simplicity
- Common view with goals and objectives
- Common understanding of capabilities and lexicons
- Alignment of efforts to ensure coherency
- Assessment to change course or direction as needed

Post event survey data and weighting would also be based on a survey of participants collected upon project completion. The realization criteria would again be determined by setting a target response to all survey questions at a score of 3 or better on a scale of 1 to 5 – a response of 3 or better would mean that there is no negative reaction to the attribute (inconclusive =1 or 2, neutral =3, possibly =4, conclusively =5).

Conclusion

In their book "Understanding Command and Control", Albert and Hayes (2006) say in a nutshell, Command and Control is about focusing the efforts of a number of entities (individuals and organizations) and resources, including information, toward the achievement of some task, objective, or goal [Ref. J]. Use of the ASIF methodology would aid in a common view and understanding of the complexity of C2 and cyber issues that we face today and in the future.

Appendix A: References

A. A Methodology to Improving Unity of Effort for Mission Partner Planning- paper 003 19th ICCRTS 17 June 2014

B. Unified Command Plan (UCP), 6 April 2011 (Under Review) (S)

C. Global Force Management Implementation Guidance (GFMIG), 15 November 2011 (S)

D. Alberts, D.S. and Hayes, R.E., 2003, Power to the Edge: Command and Control in the Information Age, CCRP, ISBN: i-893723-13-5, June 2003

E. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3110.06D Special Operations Supplement to the Joint Strategic Capabilities Plan FY 2010, 14 Sep 2012 (S)

F. National Security Strategy (NSS), May 2010

G. Joint Publication 6-0

H. NATO Defence Planning Process

I. Chairman of the Joint Chiefs of Staff Mission Command White Paper, 3 April 2012

J. Alberts, D.S., Hayes, R.E., (2006).Understanding Command and Control, CCRP Publication Series

K. ADM William McRaven, Commander USSOCOM, Posture Statement to 113th Congress Senate Armed Services Committee, Mar 2013

L. National Security Strategy (NSS), May 2015

M. ADM William Admiral McRaven, Commander, USSOCOM, SEP 2011

N. Unity of Effort Framework Solution Guide, Joint Staff, Aug 2013

O. The National Military Strategy of the United States, Redefining America's Military Leadership, 8 February, 2011

P. Joint Publication 3.0

Q. Alberts, D.S., Reiner, K.H., Moffat, J. (2010). NATO NEC C2 Maturity Model, CCRP Publication Series, 978-1-893723-21-4, 2010 Joint Publication 6-0

R. The Complete Business Process Handbook, 2015 LEADing Practice ApS

S. Improving Alignment and Unity of Effort with mission partners paper 001 – September 2016

T. NATO Defence Planning Process

U. General Dunford, Chairman of the Joint Chiefs of Staff, Dec 2015