23rd ICCRTS

"Multi-Domain C2"

A Methodology for Managing Multiple, Complex, C2-Enabling, Cybersecurity Research and Development Efforts

Topic 6: Interoperability/Integration and Security

Topic 8: Methodology, Experimentation, Analysis, Assessment and Metrics

Authors

Mr. Patrick J. Guerin
Mr. Ken D. Teske
Mr. Mark E. Miller

Point of Contact

Patrick J. Guerin
Key Management Solutions LLC
223 N Wahsatch Ave, Suite 206
Colorado Springs, Colorado 80903-2253
(719) 238-7561

Abstract

Protecting information within stand-alone systems with well-defined and static cybersecurity requirements is a relatively straightforward task. Managing and satisfying cybersecurity requirements becomes increasingly difficult as environments become more complex such as Multi-Domain C2 environments operating with multiple inter-related and inter-dependent partners (Joint, Interagency, Multinational, and Public organizations). In these environments, C2 and C2-enabling system technical, operational and policy controls both affect, and are affected by the other systems. Moreover, the cybersecurity posture is continuously adapting to mitigate evolving threat vectors so change is a constant.

In addition to these Multi-Domain C2 operational environment considerations, researchers seeking to test, develop and accelerate insertion of positively disruptive C2-enabling capabilities must purposefully strike a balance between complying with current operational cybersecurity requirements and interoperability controls (constraints) and intentionally trying to incubate, align or integrate positively disruptive C2-enabling capabilities that, in turn, affect and change current system/integrated systems technical, operational and policy controls. With so many interrelated or unknown (or to be defined) requirements, alternatives to traditional research and development environments and management approaches (such as integration platform as a service (IPaaS) or a Capability Maturity Model Integration (CMMI) variant) are needed.

This paper describes how the “Alignment, Synchronization and Integration Framework” (ASIF) and Methodology was selected to support the management of, and optimize the development of multiple, complex, C2-enabling, cybersecurity research and development efforts in a "Multiple classification and releasability, Alignment, Synchronization and Integration, Platform as a Service" (MAPaaS) environment.

Introduction

Protecting information within stand-alone systems with well-defined and static cybersecurity requirements is a relatively straightforward task. Managing and satisfying cybersecurity requirements becomes increasingly difficult as environments become more complex such as Multi-Domain C2 environments operating with multiple inter-related and inter-dependent partners (Joint, Interagency, Multinational, and Public organizations). In these environments, C2 and C2-enabling system technical, operational and policy controls both affect, and are affected by the other systems. Moreover, the cybersecurity posture is continuously adapting to mitigate evolving threat vectors so change is a constant.

In addition to these Multi-Domain C2 operational environment considerations, researchers seeking to test, develop and accelerate insertion of positively disruptive C2-enabling capabilities must purposefully strike a balance between complying with current operational cybersecurity requirements and interoperability controls (constraints) and intentionally trying to incubate, align or integrate positively disruptive C2-enabling capabilities that, in turn, affect and change current system/integrated systems technical, operational and policy controls. With so many interrelated or unknown (or to be defined) requirements, alternatives to traditional research and development environments and management approaches (such as integration platform as a service (IPaaS) or a Capability Maturity Model Integration (CMMI) variant) are needed.

In 22nd ICCRTS our team presented a very detailed paper describing research in quantum-resistant Communications Security (COMSEC) titled, "Pre-Shared Key-Enabled CSfC: A Positively Disruptive Technology and Enabler for Next Generation Mission Partner Secure Communications". [a] Since then, that ongoing Research and Development (R&D) expanded to incorporate two additional, Pre-Shared Key (PSK)-based CSfC enabling (thus C2 system and C2 enabling) RDT&E focus areas:

1) Cross Classification Domain / Releasability Boundary (CD/RB) Solutions (CCSs) – which enable Cross CD/RB monitoring and data releasability
2) C2 Agility & Approaches Enabling Dynamic Security Control Sets and Overlays [23rd ICCRTS Concept Paper 4] – which seeks to optimize the defense of C2 systems operating in dynamic environment (with varying threat vectors) by researching and developing C2-Agile overlays.

The objective of this paper is to:

1) Provide an update on the ongoing, above-mentions, cybersecurity-specific positively disruptive C2-enabling 'incubation through integration' overview of the research and development
2) Describe the "Multiple classification and releasability, Alignment, Synchronization and Integration, Platform as a Service" (MAPaaS) environment that supports these multiple, complex, C2-enabling, cybersecurity R&D efforts to include citing inhibitors we encountered in developing the cybersecurity components and MAPaaS environment
3) Describe how the "Alignment, Synchronization and Integration Framework" (ASIF) and Methodology was selected to address the identified, Cybersecurity R&D inhibitors, support

the management of, and optimize the development of the multiple, complex, C2-enabling, cybersecurity research and development efforts in the MAPaaS.

C2-enabling R&D Effort Overview

The three, primary C2-enabling 'incubation through integration' R&D efforts discussed in this paper include Quantum Resistant Commercial Solutions for Classified (CSfC), Cross Classification Domain / Releasability Boundary (CD/RB) Solutions (CCSs), and C2 Agility & Approaches Enabling Dynamic Security Control Sets and Overlays. The following sections provide an overview of each.

Quantum Computer Resistant CSfC Overview

CSfC is the United States (US) National Security Agency's (NSA's) business process for layering commercial technologies to protect classified NSS information. Because CSfC is based on commercial technologies, publicly-available ciphers and open standards, most of the information regarding CSfC is publicly available and can be found on the US NSA's CSfC website: https://www.US NSA.gov/resources/everyone/csfc/. Note that although the premise of CSfC is simple, the devil truly is in the details and there are there are many overlapping (and sometimes intentionally vague and sometimes contradictory) guidance, policies and procedures that must be addressed for each CSfC use. CSfC is founded on the principle, as depicted below in Figure 1, that properly configured, layered COTS hardware and/or software components can be specifically configured (per multiple US policy and guidance publications) to provide adequate protection of classified data in a variety of different applications.

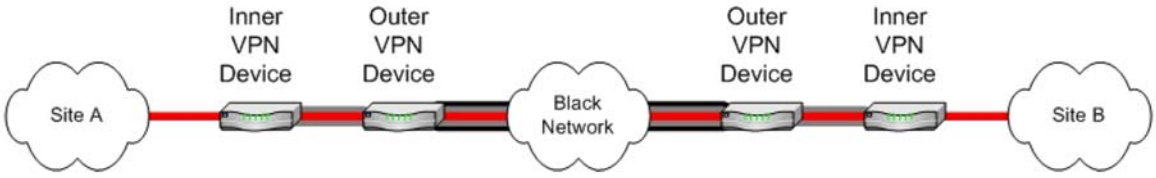

Figure 1 - US NSA CSfC Two-Tunnel Encryption

CSfC provides customers with an alternative approach to US Type-1 COMSEC for protecting classified information/systems. [b] Although the CSfC principle (layered COTS products) may be simple to understand, CSfC does force the introduction of multiple new policy, guidance, requirements and processes publications that each 'solution' must satisfy to provide the 'adequate' (Defense in Depth) protection. US NSA CSfC 'solutions' are accredited (authorized for use) by the Authorizing Official (AO) for that CSfC-enabled system or network per the US NSA CSfC Approval Process [c]. US NSA CSfC Program Management Office (PMO) does not 'accredit' a CSfC-enabled system. Rather, the US NSA CSfC PMO develops and publishes approved solution architectures called Capability Packages (CPs) that 'contain product-neutral information that will allow customers/integrators to successfully implement their own solutions. Using the information in the CPs, customers/integrators make product selections (from the US NSA CSfC Approved Components List [d]) while following the guidelines / restrictions to create an architecture with specific commercial products configured in a particular manner'. [e]

In terms of registering a proposed NSA CSfC CP-based solution for use, the end customer develops, self-tests against CP-specific requirements, and registers the solution with the US NSA CSfC PMO. In the past, the US NSA CSfC PMO could quickly review and register a customer-developed solution that was 100% compliant with a CP. If, however, a customer-proposed solution is not 100% complaint with a CP then the customer must request a deviation approval from US NSA which, in addition to adding delay to the approval process, entails the customer (and potentially US NSA) performing a risk analysis against the unsatisfied US NSA CSfC CP requirements and a proposal of short and long-term mitigations. Unfortunately, ALL current CSfC solutions employing only certificate-based encryption require deviations for one reason or another. As will also be explained, employing one or two PSK-based encryption tunnels mitigates and resolves these deviations.

Capability-specific CPs provide a general, CSfC capability description, detailed information related to the CP's security architecture, a listing of eligible, CP-specific products, security roles of the products, system security requirements/guidance for customers/integrators, administrators, testers, certifiers/accreditors, interoperability, key management, and lifecycle maintenance. Currently, four US NSA CSfC CPs have been approved [f] and include:

1. Mobile Access (MA) v2.0 CP which describes how to protect classified data in Mobile Access Solutions transiting Wired Networks, Domestic Cellular Networks, and Trusted Wireless Networks to include Government Private Cellular Networks and Government Private Wi-Fi networks
2. Campus Wireless Local Area Network (WLAN) v2.1 CP which enables customers to meet the demand for commercial End User Devices (i.e., tablets, smartphones and laptop computers) to access secure enterprise services over a campus wireless network
3. Multi-Site Connectivity (MSC) v1.0 CP uses two nested, independent encryption tunnels to protect the confidentiality and integrity of data as it transits the untrusted network. The two encryption tunnels protecting a data flow can use either Internet Protocol Security (IPsec) generated by a Virtual Private Network (VPN) Gateway or Media Access Control Security (MACsec) generated by a MACsec Device
4. Data-at-Rest (DAR) v4.0 CP which enables customers to implement two independent layers of encryption providing protection for stored information using US NSA approved cryptography while the End User Device is powered off or in an unauthenticated state.

The CPs generally follow the same format but do provide CP-specific network and reference diagrams. Figures 2 and 3 provide examples of CP-specific diagrams.

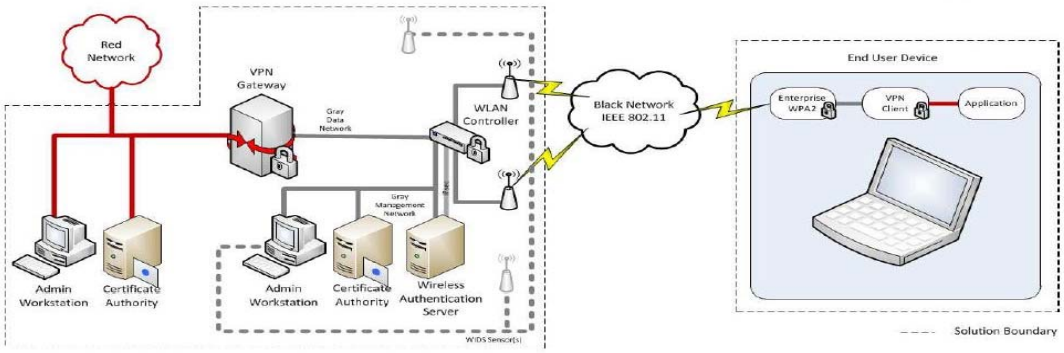

Figure 2 - Campus WLAN Infrastructure for Classified

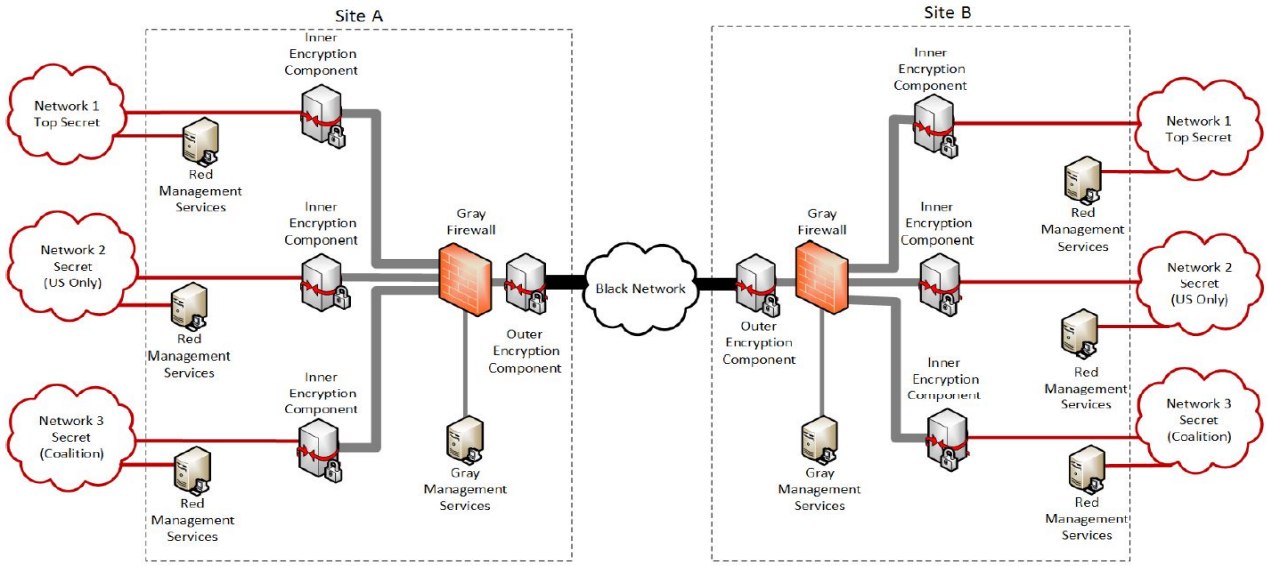

Figure 3 - MA CP Solution Continuous Monitoring Points

As noted by the different CP versions and driven by new customer requirements (and/or a trend in specific CP deviation requests), over the years CSfC CPs have been newly released, modified / evolved, and in some cases, been cancelled. Again, driven by unique customer requirements that could not be optimally satisfied by traditional US Type-1 COMSEC, the Operational View-1 (OV-1) depictions in Figures 4 and 5 are two examples of previously-accredited, 'positively disruptive' US systems / networks that pushed the envelope (at that time) and set precedence (by both obtaining an Authority to Operate (ATO)) that eventually affected the CPs that exist today.

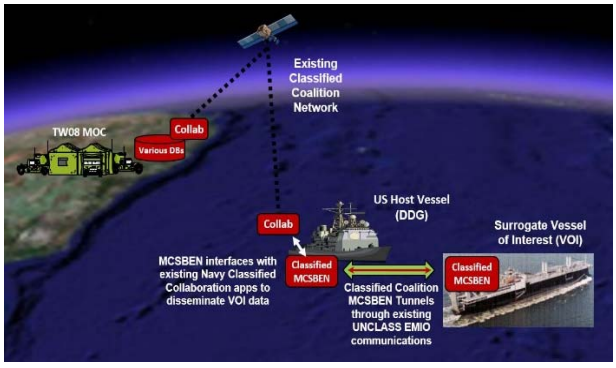

Figure 4 - MCSBEN OV-1

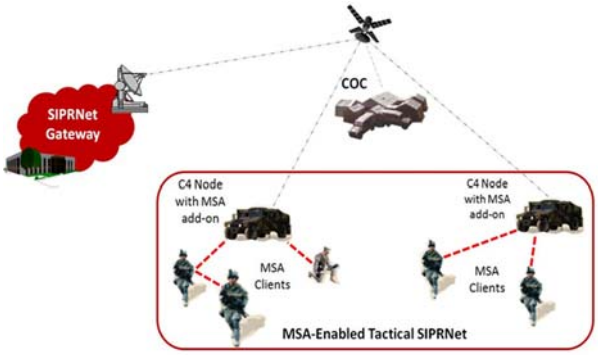

Figure 5 - MSA OV-1

- **Maritime Domain Awareness (MDA) Coalition Suite B Enabled Network (MCSBEN)** was a US 3rd Fleet-sponsored, Trident Warrior 2008 (TW08) research effort exploring data sharing / collaboration capabilities between Expanded Maritime Interception Operation (EMIO) On-Scene Commander (OSC)-Designated Operator (EODO) on a US Host Vessel Classified Coalition LAN and Vessel of Interest (VOI) boarding party. [g]

- **Mobile Secure Architecture (MSA)** was a US Office of Naval Research (ONR) funded effort to research, design, implement, test and accredit a lower-cost, COTS-based, US NSA

Suite B-enabled, non-Controlled Cryptographic Item (CCI) Wi-Fi add-on communications capability that extends tactical SIPRNet with reduced operational controls compared to traditional Type-1 (CCI) COMSEC. [h]

One (if not the most) critical aspects of CSfC is it's use of commercial cryptographic algorithms and self-generated keying approach. The original commercial cipher suite for classified announced by US NSA in 2005 was 'Suite B' and was comprised of [i]:

- Advanced Encryption Standard (AES) with keys sizes of 128 and 256 bits for symmetric encryption
- Secure Hash Algorithm (SHA-256 and SHA-384) for message digest
- Elliptic-Curve Menezes-Qu-Vanstone (ECMQV) for key agreement
- Elliptic-Curve Diffie-Hellman (ECDH) for key agreement
- Elliptic-Curve Digital Signature Algorithm (ECDSA) for digital signatures

Driven by customer requirements, starting on 2012 US NSA CSfC PMO modified the Suite B cipher suite. The cipher suite was again revised in 2016 to mitigate threats introduced by quantum computers.

Unlike traditional digital computing that requires that the data be encoded into binary digits (bits), each of which is always in one of two definite states (0 or 1), quantum computation uses quantum bits (qubits), which can take advantage of quantum physics phenomena such as superposition and entanglement, to perform operations on data at an exponentially faster speed than the best known classical strategies, rendering some forms of modern cryptography powerless to stop a quantum codebreaker.

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	----------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

Table 1 Impact of Quantum Computing on US NSA CSfC Algorithms

Quantum factoring algorithms pose a legitimate, considerable threat to security. This is because the most common form of internet security, public key cryptography (under which the Suite B Elliptical curve ciphers fall), relies on certain math problems like factoring numbers that are hundreds of digits long being effectively impossible to solve.

Table 1 (above) from the US NIST Report on Post-Quantum Cryptography [j] outlines the impact of quantum computing on the US NSA CSfC Suite B algorithms. In line with the NIST findings, in December 2015 the US NSA Information Assurance Directorate (IAD) announced that the

'continued progress in the research of quantum computers has made it clear that elliptical curve cryptography [which comprised the core of the 'non-interim, certificate-based CSfC Suite B cipher suite] was not the long-term solution that many had once hoped it would be. Thus, we have been obligated to update our strategy. [k]

In January 2016 the US NSA CSfC Program 'evolved' from 'Suite B' to the Commercial National Security Algorithm (CNSA) Suite [l] and removed the lower requirement set for US Secret and defined one set of requirements for 'Up to Top Secret' (requiring larger key sizes and extended algorithm parameters), and dropped the 1 October 2015 deadline to stop using RSA and allowed for use of DH 3072bit modulus.

Although extending the CNSA algorithm parameters may increase COMSEC for 'short life' data, per Table 1, the US NIST does not consider PKI (or certificate based encryption) secure. As is often overlooked, the threat of reverse factoring against certificate-based encrypted data doesn't start in the future when quantum computers are more powerful, rather, if an adversary can passively collect certificate-based encrypted data now they will be able to retroactively decrypt all collected data once the quantum computers become powerful enough. This is of concern to the US because 'National Security information intelligence value is often 30 years (sometimes more)' [m] which is why the US NSA's CSfC guidance for long intelligence life data is to implement a layer of quantum computer resistant protection. 'Such protection may be implemented today using large symmetric keys and specific secure protocol standards CSfC deployments involving an IKE/IPsec layer may use RFC 2409-conformant implementations of the [Internet Key Exchange] IKE standard (IKEv1) together with large, high-entropy, pre-shared keys and the AES-256 encryption algorithm.' [k]

More clearly stated, AES-256 using PSK is quantum computer resistant and any PKI or certificate-based algorithm that relies on factoring (elliptical curve, ECDH, DH, RSA) is not quantum computer resistant.

When discussing PSK CSfC, it is important to not simply limit the scope of research and activities to only addressing the problems at hand (trying to simply add a PSK-enabled, AES tunnel to existing US CSfC solutions to address quantum computer threat). PSK research and eventual development has a high probability of not only being positively disruptive to US CSfC for the US NSSs but also for all Mission Partners and beyond because, in the long term, the world needs to find new, non-PKI/certificate-based authentication and encryption key generation technologies and methods without revering to Type-1-like encryptors.

Although just scratching the surface, Figure 6, 'Evolution and Forecast of the US Cryptographic Options' provides a high level visual history and trajectory of several potential and probable research areas related to PSK CSfC (again, for both US NSS and Mission Partner Environments). It also illustrates how these R&D areas have and will affect or be affected by other research areas as we move forward in this complex and intertwined RDT&E realm. Using this depiction, our team's R&D area of focus is within the (top right) superimposed arrow titled "Post Quantum (PQ) World" with an emphasis on optimally moving from Suite B (EC Certificate & PSK-Based) to PSK-based CNSA ciphers. Outputs of this focused R&D is essential because RSA and Certificated-based CNSA cryptographic CSfC is not secure per US NIST and face obsolescence.

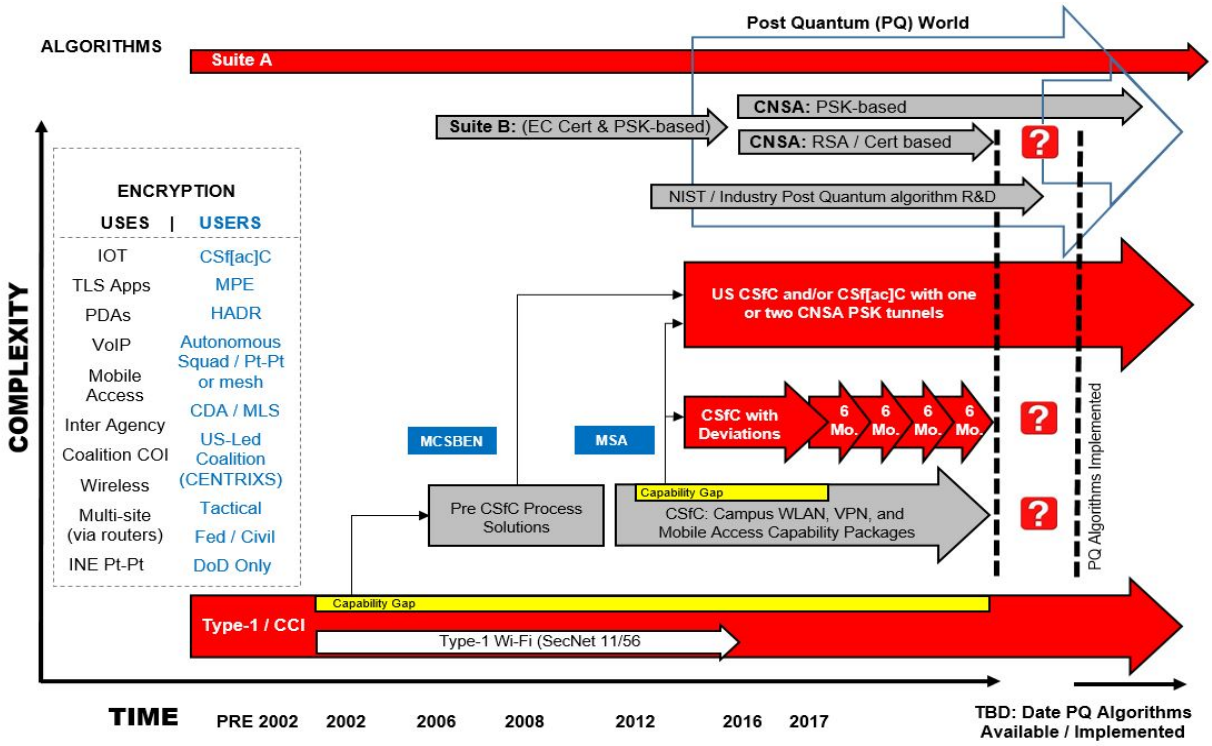

Figure 6 - Evolution and Forecast of the US Cryptographic Options

Cross Classification Domain / Releasability Boundary (CD/RB) Solutions (CCSs)

Our team's second, C2-enabling cybersecurity effort involves R&D of technologies and techniques to securely pass data from one security classification or releasability to another. Examples include, but are not limited to, passing data between US Unclassified to Secret networks (different security classifications) or between US Secret and NATO Secret networks (Same classification but different releasability requirements (RELs)). Figure 7, from an US NSA Multi-Site Connectivity CSfC CP, illustrates the requirement for a cross domain solution (CDS) capability to support aggregation of network monitoring data from one network classification to another.

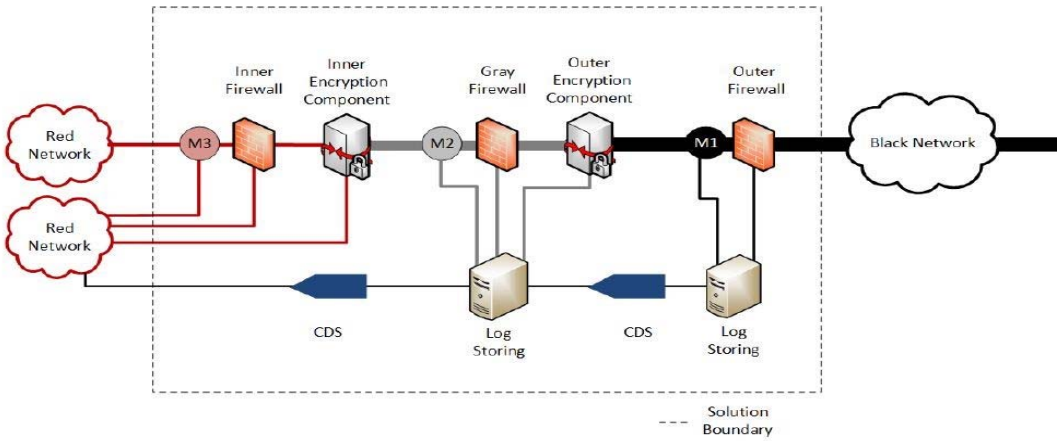

Figure 7 – US NSA CSfC MSC CP-Defined Monitoring Points

Although the US NSA CSfC PMO states, "The advantages of consolidated monitoring at all three points are fully realized when data from all devices is collected within the Red monitoring enclave using a CDS and event correlations", the Mobile Access (MA) CP states, “The requirements for a CDS capable of providing separation between enclaves of two or more classification levels are outside the scope of this CP.” Through this, the US NSAUS US NSA CSfC PMO is distancing the CSfC approval process from discussions of employing a CDS. This is because CDSs are expensive (from both a financial and time to implement perspective) and many times overkill – especially for one-way connections. The Cross-Classification Domain / Releasability Boundary (CD/RB) Solutions (CCSs) R&D – which has direct applicability to C2 systems operating in a Mission Partner Environment (MPE) – attempts to address this issue.

As is the case with CCIs, US CDSs cannot be exported to/employed by Mission Partners. Data Diodes and Controlled Interface (CI) systems can be used instead of a CDS. Data Diodes are hardware-based cybersecurity devices that physically enforce a one-way flow of data. Data diodes are used as cybersecurity tools to isolate and protect networks from external cyber threats, prevent penetration from external resources and, in Controlled Interface (CI) systems, provide one way “assuredness”. Figure 8 depicts one, on-going (C2 and C2 system-enabling) CCS R&D capability. Prototype operations (numbers below map to numbers in yellow circles in figure) include:

1. Dedicated Client Subscriber* on each network pulls data from local/remote-hosted sources and/or subscribes to specific network data feeds
2. All Client-specific data is passed via one-way tap to IDS Collector, which forwards data from ALL client Subscribers to an IDS ‘Command Post’
3. Specific collected data is forwarded ** via one-way tap *** to Consuming System (CS) for ingestion

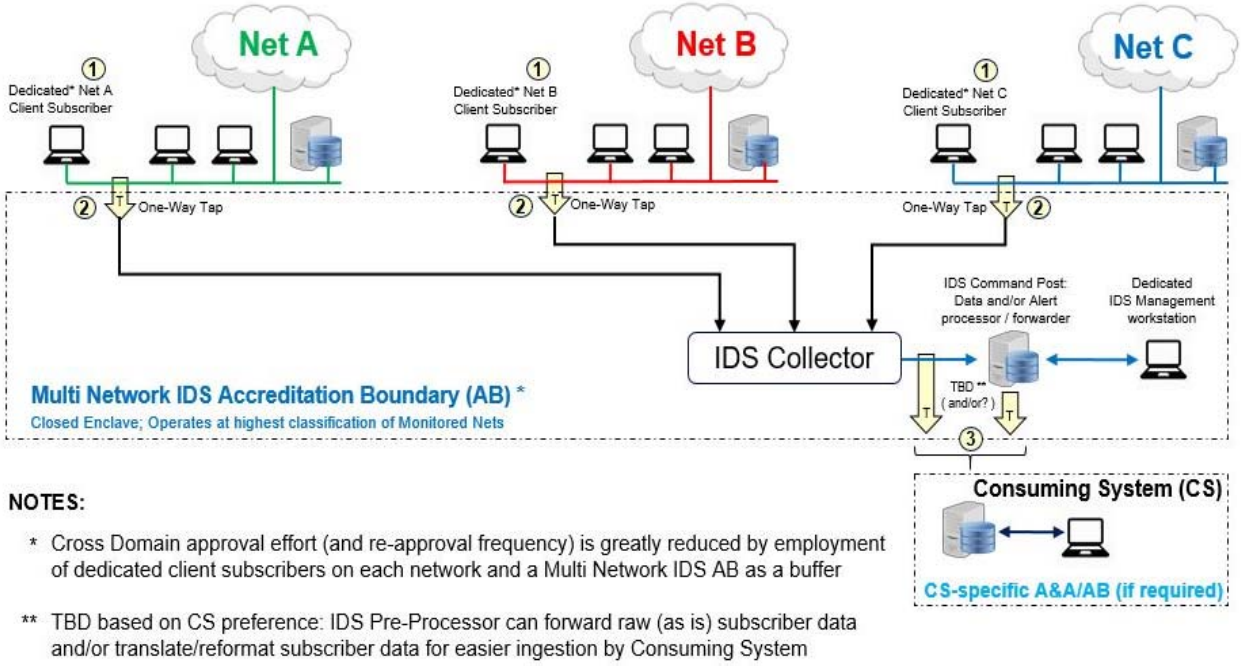

Figure 8 – CCS RDT&E Prototype Example

C2 Agility & Approaches Enabling Dynamic Security Control Sets and Overlays

Our team's third cybersecurity R&D effort, C2 Agility & Approaches Enabling Dynamic Security Control Sets and Overlays [ICCRTS 2018 Concept Paper 4 submission], seeks to optimize the defense of C2 systems operating in dynamic environment (with varying threat vectors) through research of the possibility of leveraging Agile C2 approaches to define notional system operational use cases and associated threat vectors to support the research and developing of Agile C2-related security control overlays which would support the variety of missions, circumstances, and the collections of entities needed to meet these security challenges.

Prior to connecting a new personal computer to a network for the first time, a typical user will first apply security controls such as changing the default passwords, installing antivirus and setting access permissions. The same generally holds true for new systems being adding to corporate, federal and Defense networks: Security controls are applied based on the value of the data being protected to defend against the probable threats against that data. The perpetual questions facing all data owners and administrators of these computer systems are, 'How many controls, and to what degree of strength, are adequate?"

An overall network is only as strong as its weakest link. Because security controls were being inconsistently implemented at the system level - which introduced network-wide vulnerabilities - in March of 2014, the US Department of Defense (DoD) issued Instruction (DoDI) 8510.01 "Risk Management Framework (RMF) for DoD Information Technology (IT)". [n] This Instruction defined a process for identifying and assessing the implementation of individual security controls and overlays (pre-defined 'one size fits all' sets of security controls), and the tailoring of these security controls and overlays resulting in a static, system-specific set of security controls. Unfortunately, after four years of RMF, the same questions as to which security controls are minimally required or optimal for an operating environment are still largely unanswered. Moreover, aside from an 'apply all controls for a worst-case scenario' approach, RMF does not address how to handle systems - such as Command and Control (C2) systems - that operate in changing/evolving environments with changing/evolving threat vectors, and there does not appear to be a plan to explore either of these problems.

C2 Agility Theory states that there is no "one-size-fits-all" approach to C2 that is appropriate for all missions and circumstances. Given the variety of missions, circumstances, and the collections of entities needed to meet these varied challenges, there is no single approach to C2 that is appropriate for all of these situations. Therefore, NATO, member Nations, and partners will need to be able to employ more than one approach to C2, understand when different C2 Approaches are appropriate, and have the ability to efficiently transition between and among C2 Approaches in a timely manner. [o] If this is true, then it stands to reason that the Agile C2 operations-supporting systems will face varying threat vectors over time and would require more than one (perhaps many) security controls sets/overlays to adequately protect them… but again, *which* security controls sets/overlays.

RMF Step 1 requires system/data owners to categorize the system and the information processed, stored, and transmitted by that system based on an impact analysis and define the system's

Confidentiality, Integrity, and Availability (C, I, A) values separately as being Low (L), Moderate (M) or High (H) such that the result is system characterization variables (C ([L, M, H]) I ([L, M, H]) A ([L, M, H])). Figure 9 illustrates the 27 'standard' security control set space options and depicts two representative system Impact Assessment results (Black system = (C(L) I(L) A(L)) and Yellow system = (C(H) I(H) A(H)) for the three (C, I, A).

Per RMF, in Step 2 system/data owners select an initial set of baseline security controls for the system based on the security categorization, tailoring and supplementing the security control baseline as needed based on organization assessment of risk and local conditions [p]. While this may sound straightforward, there are numerous options and devil is in the details. Each control set (for example, the black (LLL) cube or yellow (HHH) cube in Figure 9) has on average about 500 impact assessment-specific controls that need to be applied to a system. This is before tailoring.

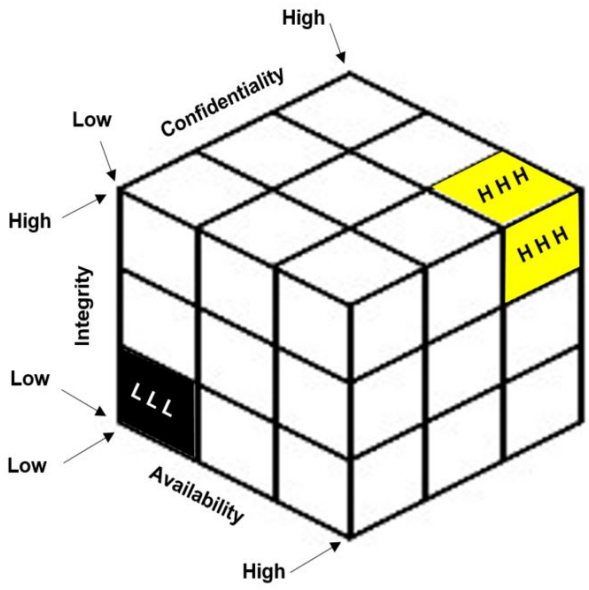

Figure 9 – Impact Assessment Result Space

Because one size doesn't fit all, RMF allows system/data owners to apply, remove, and increase strength or decrease strength of individual controls within the default control set. Unfortunately, this tailoring can not only lead to cases where the resulting security controls are too strict or lenient, but more importantly lead to inconsistencies such as two similar systems in the same operating environment having different controls resulting is increased risk to interconnecting systems.

To minimize this occurrence, the US DoD established the 'overlay', which is a specification of security controls and supporting guidance used to complement the default (impact assessment-determined) security control baselines and parameter values. "Overlays may be applied to reflect the needs of different information types (e.g., personally identifiable information [PII], financial, or highly sensitive types of intelligence); system functionality needs (e.g., stand-alone systems, cross domain solutions, or controlled interface systems); or environmental or operationally-driven needs (e.g., tactical, space-based, or test environment)." [p] Current overlays include:

1. **US National Security System-Specific**: Cross Domain Solutions, Space Platform Intelligence (which are For Official Use Only (FOUO)), Classified Information, and Privacy,
2. **Functional Mission-Specific**: Nuclear Command and Control, Communications Systems Overlay. [q]

Although overlays (which leverage the 'one size fits all' concept) were intended to aide in establishing more consistent baselines, problems still exist. First, guidance on applying overlays is counter-productive. DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk

Management Framework (RMF) into the System Acquisition Lifecycle [p] states, "It is mandatory to identify and use all appropriate overlays, but it is not mandatory to comply precisely with all specifications in all overlays, as even the overlays were developed based on a set of assumptions that may or may not apply to all systems using the overlay. That is, further tailoring of the overlay specifications is often required; this is system-specific tailoring, and the rationales for selecting or de-selecting the controls must be documented in the [System Security Plan] for Authorizing Official (AO) approval." Secondly, overlays are based on static operational use, thus they can only provide adequate defense against a static operational threat. Systems employing static overlays creates vulnerabilities to self and interconnecting systems as mission (and threat vectors) expand into distributed mission sets. To be effective, either the existing overlay approach needs to be revised to provide more operational granularity and support of dynamic operating environments, or an alternative set of overlays, based on Agile C2 Approach-like operating environments, needs to be made available to system/data owners.

The NATO Network Enabled Capability (NEC) C2 Maturity Model (N2C2M2) [r] defines five C2 approaches (depicted in Figure 10), ranging from Conflicted C2 to Edge C2, that correspond to different regions within the C2 Approach Space. Agile C2 "is the ability to recognize which C2 Approaches are appropriate for the situations (e.g., mission, operating environment, and set of coalition partners or contributing entities) and dynamic transition to these." [r] It is from this reference we make our Security Control Overlay propositions.

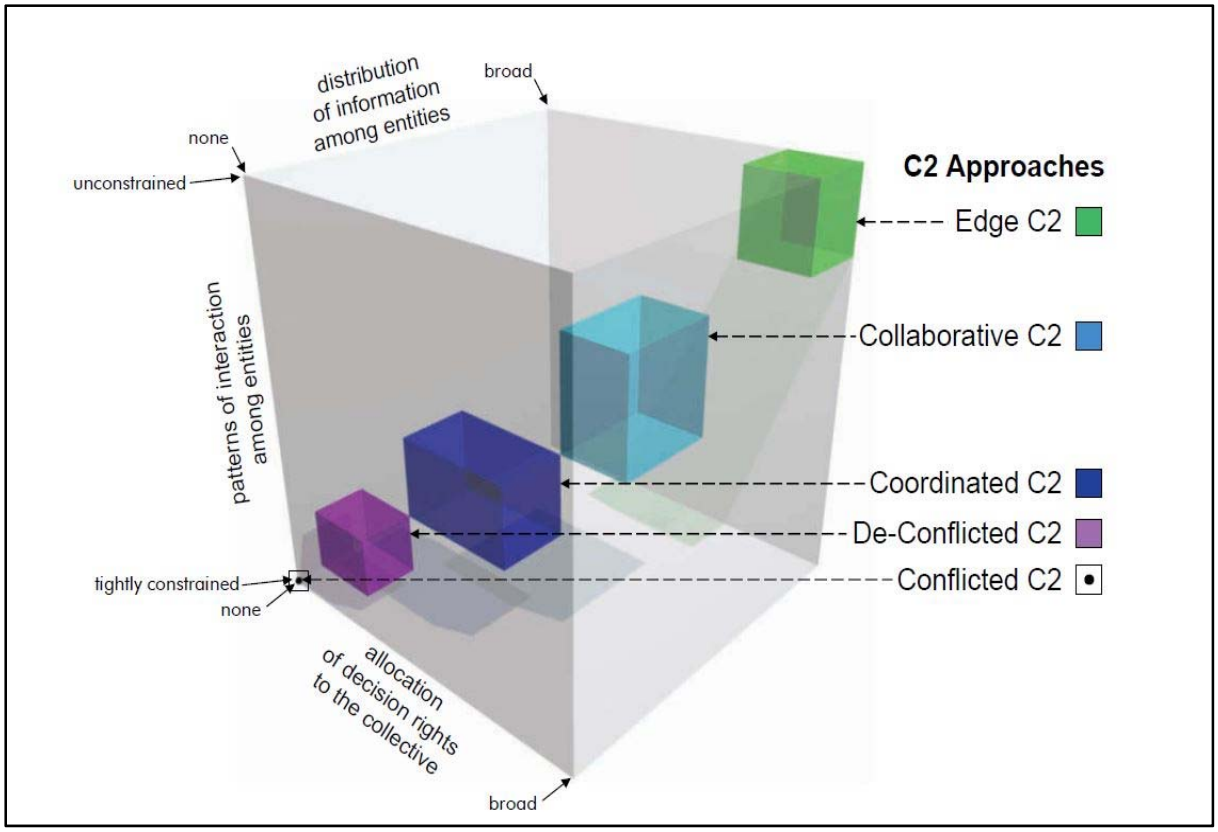

Figure 10 – C2 Approaches as regions in the C2 Approach Space

Although other approaches are under consideration, the two, primary approaches to the overlay development research are:

1) Develop Agile C2 Approach-Based overlays: Involves developing five new overlays based directly on each of the five C2 Approach areas
2) Develop Agile C2 Approach-Enabling overlays: Involves developing new overlays based, not on traditional C, I, A attributes, but on new x, y, z coordinates that enable (but do not directly mirror) the five C2 Approach areas.

MAPaaS Environment Overview

The previous sections of this paper provided an update on the three, ongoing, cybersecurity-specific positively disruptive C2-enabling 'incubation through integration' R&D efforts. This section describes the "Multiple classification and releasability, Alignment, Synchronization and Integration, Platform as a Service" (MAPaaS) environment that supports these multiple, complex, C2-enabling, cybersecurity R&D efforts – to include identifying inhibitors we encountered in developing the cybersecurity components and MAPaaS environment.

Prior to 2016, our team's cybersecurity R&D focus was on (non-quantum resistant) certificate-based CSfC. Supporting this only required a single entity (company) implementation of a hub and spoke-based network to test 'tunnel within tunnel' encryption technologies and techniques. As illustrated in Figure 11, the prior lab environment was composed of multiple "Jaw Breaker" (JB) layers that employed increasing security measures (tunnels within tunnels) based on a surrogate system/data Mission Criticality assessments and development effort classification requirements.

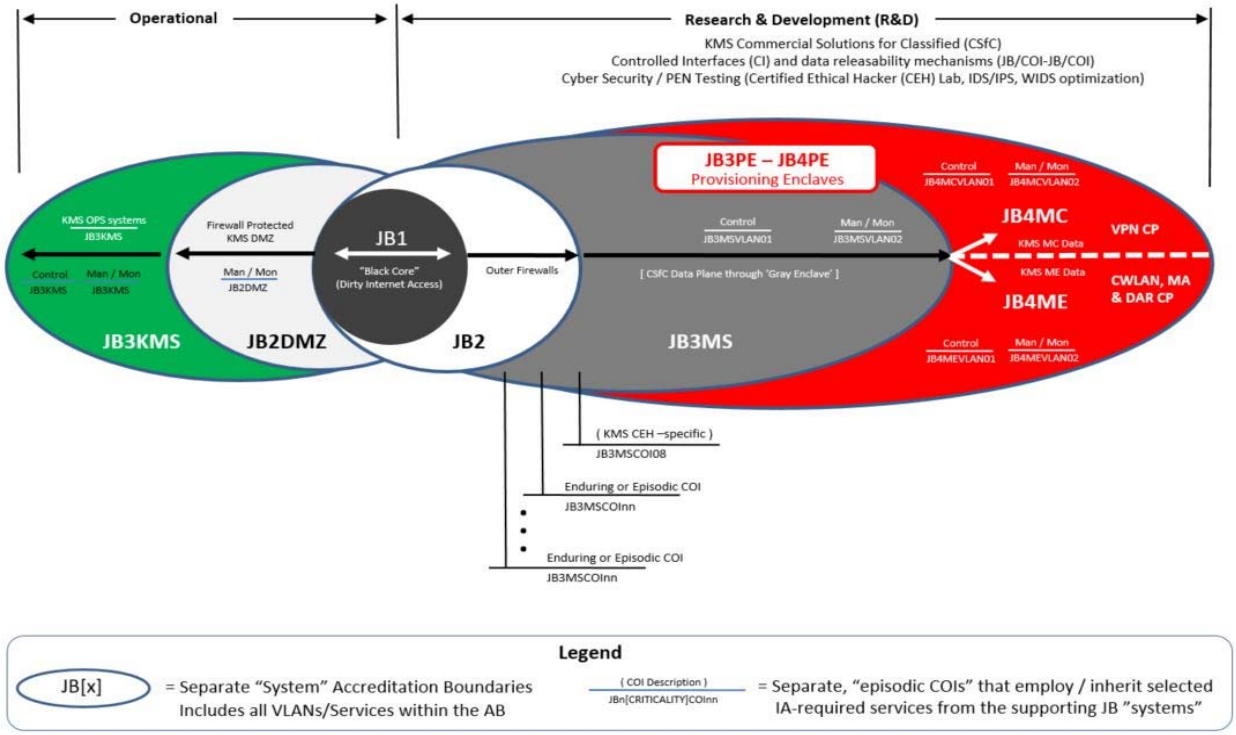

Figure 11 –Jawbreaker (JB) Tunnel within Tunnel Layers and COIs

Jaw Breaker layer control sets included US National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-171 Rev.1; Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations, NIST SP 800-53 Rev. 4; Security Controls and Assessment Procedures for Federal Information Systems and Organizations, and North Atlantic Treaty Organization (NATO) Document AC/35-D/2004-Rev. 3; Primary Directive on Communication and Information System Security, 15 Nov 2013 directives as a baseline. Each JB layer inherits and/or provides inheritance of cybersecurity services to other JB layers. Extending from the JB layers (and inheriting any number of IA services) are separate Community of Interest (COI) network enclaves. The overall MAPaaS encompasses many separate, episodic and enduring, overlapping and/or shared network management capabilities based on different Assessment and Authorization boundaries that may or may not involve many separate cybersecurity-related services, controls, and/or control inheritance, thus why aligning these requirements is essential.

Engineers on our team had been developing and deploying CSfC COMSEC solutions since 2006 and relied on the Capability Maturity Model Integration (CMMI®) for Services Version 3.1 to manage individual JBs/COIs within the overall environment. Because the initial CSfC standards and requirements (which were the primary drivers of this environment) were well defined and static, CMMI for Services was adequate for managing the environment. However, when NSA made the announcement in 2016 to move from certificate-based encryption to quantum resistant CNSA-based encryption they not only changed the focus of many US cryptographic R&D entities' RDT&E efforts, but more importantly changed many of the CSfC requirements to "to be determined". This forced a re-evaluation and additional research of how best to manage a more dynamic and 'incubation focused' R&D Learning Environment (LE) that was extended to include external entities (other Integrators, manufacturers, US Service Labs and customers).

In the pre-quantum world, our R&D environment was more hub and spoke (with an emphasis on integrating the spokes into the hub-defined standards and interfaces). Our post quantum R&D environment, which now added the complexities of Cross Classification Domain / Releasability Boundary (CD/RB) Solutions and C2 Agility & Approaches Enabling Dynamic Security Control Sets and Overlays R&D efforts, required an emphasis on effort alignment over absolute integration. The environment still needed to provide an integration capability to support existing, static CSfC standards and solutions, but also needed to provide a new, in parallel, more agile (less restrictive) environment that enabled "out of the box" thinking and development that could also support the alignment or integration testing of those "out of the box" capabilities with the more mature standards and technologies.

As depicted in Figure 12, The Evolved R&D Environment, the original (gray / outer tunnel) hub and spoke-based R&D environment expanded to include and interconnect multiple, separate R&D partner/participant sites. By then employing (red, blue and orange) inner CSfC tunnels, which created logical site to site connections, we provided environment participants the ability to participate in a single or multiple cybersecurity R&D efforts and events.

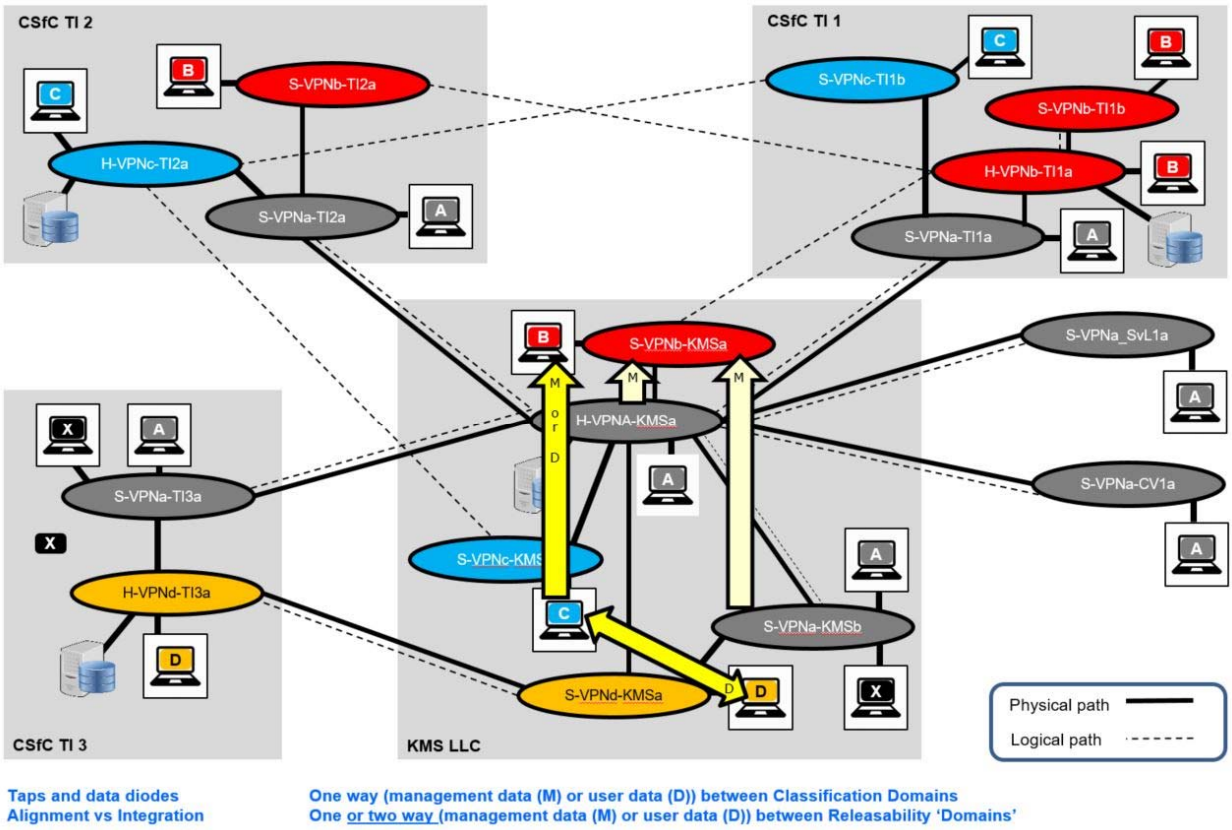

Figure 12 – The Evolved R&D Environment

Figure 12 illustrates how the various networks and enclaves are physically and logically separated (with Memorandum of Agreement (MOA)-defined entrance requirements to enforce releasability controls). The yellow (one and two-way) arrows illustrate how the intentionally separated COIs/environment are technically capable of supporting RDT&E for quantum resistant CSfC, Cross Classification Domain / Releasability Boundary (CD/RB) solution, and C2 Agility & Approaches Enabling Dynamic Security Control Sets and Overlays R&D.

We found several inhibitors to effectiveness (that are probably present and affecting most C2-enabling R&D environments) became apparent as this Multiple classification and releasability, Alignment, Synchronization and Integration, Platform as a Service (MAPaaS) environment grew:

- **Differing lexicon, taxonomy, or language**: Each of the MAPaaS participants brought into the environment their own set of R&D, systems and process terms or -in some cases - unique interpretations of generally accepted terms. For example, organizations who had been employing International Organization for Standardization (ISO) 9001 Quality Management Systems (QMS), Capability Maturity Model Integration (CMMI) for Development or Services, or the US NSA Information Assurance Technical Framework (IATF) each had their own set of process terms

- **Confusion over mixed messages**: Examples include (a) from a requirement source (example: US NSA stating that CSfC 'supports coalition partners', however the fine print is "if the US command owns the network and assumes the residual risk" and "may only include 5-EYES nations", and (b) initially-stated R&D team's objective of the CSfC R&D environment ("Collaborate on, and test quantum-resistant PSK-based CSfC." What exactly does this mean?)

- **Silos of information (lack of sharing)**: Not all the participants were fully compliant (in their development or operational environments (passing Controlled Unclassified Information (CUI)) with NIST 800-171r1 or US NSA CSfC PMO MOA requirements for protection of CUI so not all sensitive R&D information could be shared (which inhibited the overall learning environment by excluding participants)

- **Lack of interoperability**: Although CSfC employs general availability, open standards-based commercial products, one vendors products generally would not be fully interoperable with another vendor's products of the same type. This was most often the case when trying to integrate advanced (and generally more proprietary) vendor monitoring and management capabilities

- **Conflicts in planning timelines**: Although no party was intentionally dragging their feet, there were conflicts as to how fast a 'solution' could be developed (relative to how many and what type of resources could/should be provided by participants). Whereas existing (quantum computer vulnerable CSfC deployments) wanted a stop-gap/quick fix (anything is better than nothing) technical capability, others were looking for a long term, enterprise supporting solution (which would take more time to do it right)

- **Competing priorities**: Also related to the previous bullet, most participants were more interested in providing one manufacturer-specific CSfC service/capability/function or focusing on one CSfC Capability Package (Campus WLAN, Data at Rest (DAR), Mobile Access (MA) or Multi-Site Connectivity (MSC) CP or a CP set. Most R&D-centric organizations (US national Laboratories and this Paper's authors) were focused on draft CPs and more interested in developing new CPs and prototyping capabilities, whereas most COTS product manufacturers and other CSfC Trusted Integrators (TIs) were most (only in some cases) interested in tangible items they could sell at present

- **No established process (everything is ad hoc)**: There is no single process all could follow. Worse than as stated above (that many participants brought their own process), the larger problem was that most participant (per their organizational policies) were required to follow their self-defined process which made 'all must follow the host organization's process' an unsuccessful approach

Figure 13, Representative Conversations in the Previous R&D Environment, illustrates many of the above-cited inhibitors which resulted in participant 'talking past' each other and inefficiency.

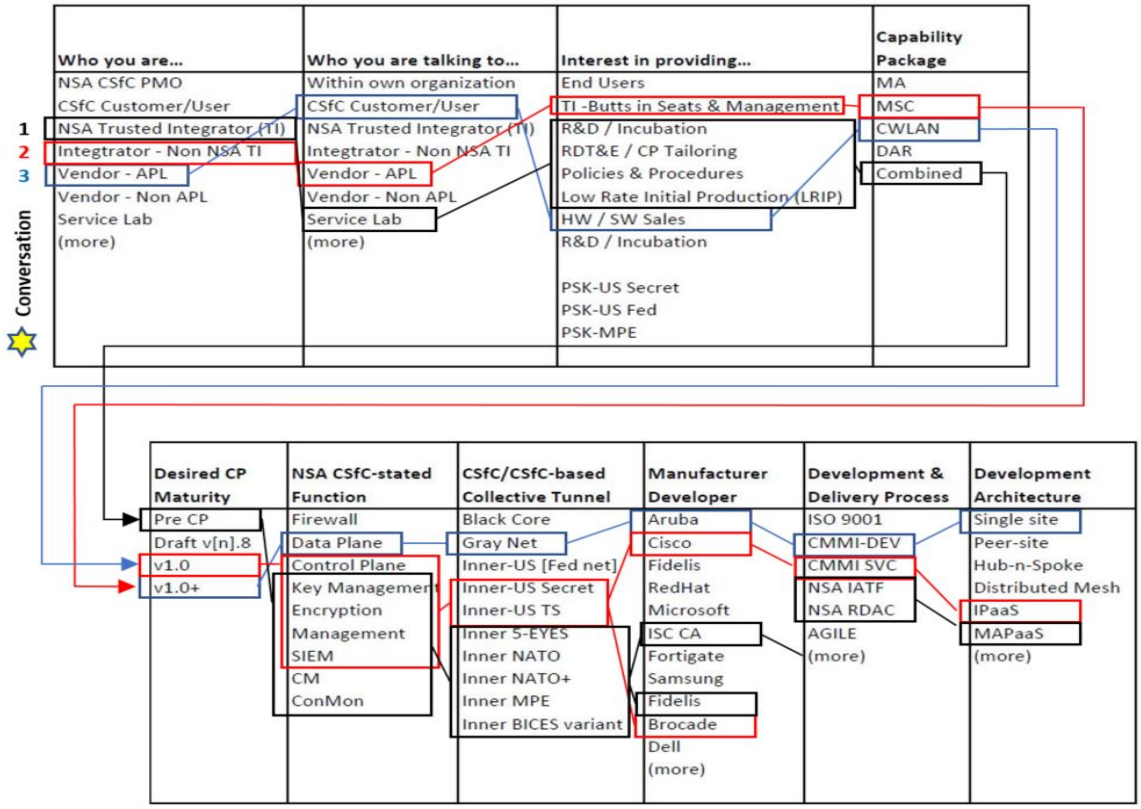

Figure 13 – Representative Conversations in the Previous R&D Environment

Releases in early 2018 of updated DAR, Campus WLAN and MSC CSfC CPs by US NSA, along with a new list of approved CSfC components, offered the opportunity to reset and re-align the overall R&D environment. Although a longer-term organizational and self-assessment of the environment's activities and inefficiencies was planned (which was the first step in developing a new plan ahead), shortly after kickoff it quickly became apparent that the initial MAPaaS Environment's inefficiencies were the result of allowing over half of the most common inhibitors to Unity of Effort' (Table 2) to occur.

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 2 – Common Inhibitors to Alignment or Unity of Effort

Based on this finding, and after first obtaining concurrence from the US NSA CSfC PMO to employ it in support of US NSA CSfC PSK-based RDT&E, the cybersecurity R&D environment stakeholders on our team initiated the application of the Alignment, Synchronization and Integration Framework (ASIF) and Methodology [r, s, t, u, v] to address the identified Cybersecurity R&D inhibitors, support the management and optimization the development of the multiple, complex, C2-enabling, cybersecurity research and development efforts in the MAPaaS.

The Alignment, Synchronization and Integration Framework (ASIF) and Methodology

Based on a Unity of Effort (UoE) framework that began as the Planning Synchronization Framework which was a conceptual approach to visualize components of existing plans, programs, and activities to improve the distribution and application of scarce resources with maximum positive effect, the ASIF and Methodology was specifically developed to address the common inhibitors to unifying efforts. [r, s, t, u, v] With Framework and Methodology stages depicted in Figure 14, the repeatable and reusable ASIF and Methodology includes the structure, definitions, templates, and how-to instructions to manage and enable the multiple, complex, C2-enabling, cybersecurity research and development efforts and the overall MAPaaS environment based upon these four principles:

- Common understanding of the situation
- Common vision, goals and objectives for the mission
- Coordination of efforts to ensure continued coherency
- Common measures of progress and ability to change course or direction as needed

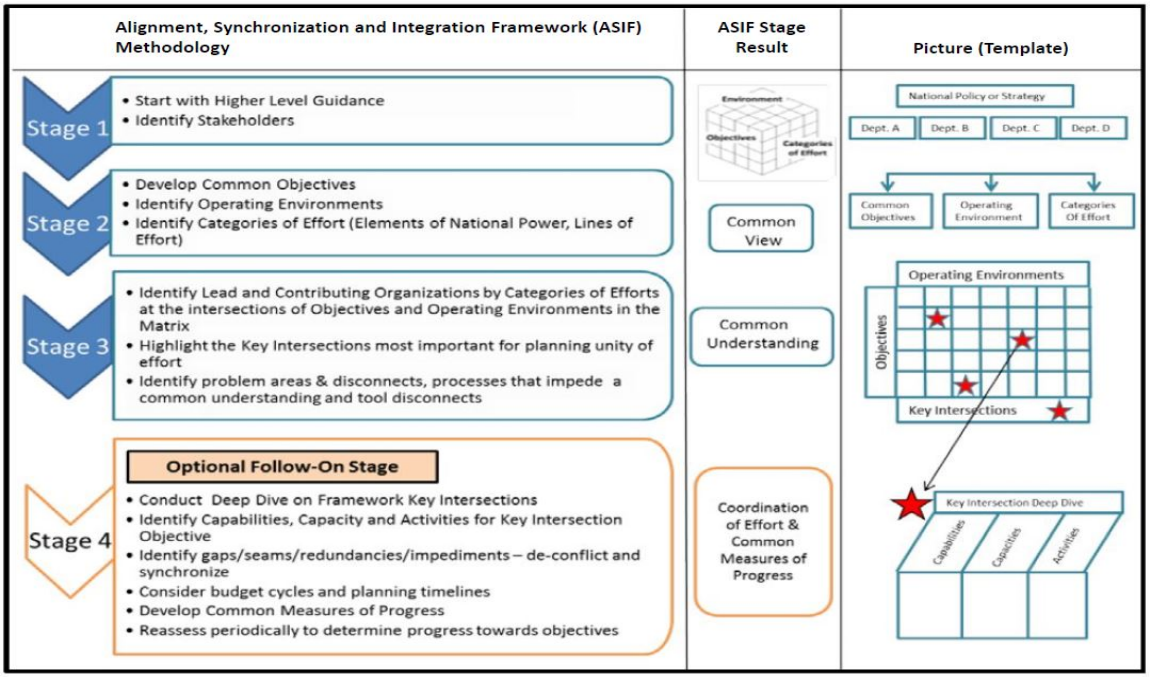

Figure 14 – ASIF Methodology Stages

ASIF employs a repeatable pattern to align multiple stakeholders with various portfolio, projects and programs. It creates a consistent and institutionalized approach to align, plan and resource programs and projects towards meeting common strategic objectives, expectations and requirements. ASIF improves alignment within planning, investments and synchronization of effort across multiple portfolio, projects and programs, departments, interagency and resources. It enables alignment for complex planning efforts, and reduces duplications of efforts across business, application and or technology areas. It standardizes and integrates complex topics for

better benefit Realization, improves joint delivery and execution, enables better transparency and traceability, and – perhaps most importantly - does not disturb existing efforts, rather, it will provide a means to inform, integrate, synchronize and control.

The most important difference between the ASIF and Methodology and other approaches to US Government or other entity planning is that each organization can continue to operate using their own planning and programming processes while mapping to a common Framework. To apply the ASIF and Methodology, stakeholders must meet, must communicate, and must collaborate to gain consensus of a common view and common understanding of the situation. These "consensus" gathering meetings, by their very nature, improve unity of effort and may be the most important part of this process. The foremost goal is to create a common understanding of who is doing what, where, and when in the area of importance to work together to improve unity of effort towards meeting agreed upon goals and objectives.

In 2016 this team continued the evolution of the UOE Framework to the Alignment, Synchronization, and Integration Framework (ASIF) in order to directly support bridging of an existing capability gap, that both United States Special Operations Command (USSOCOM) J3-International directorate and North Atlantic Treaty Organization (NATO) Special Operations Forces (SOF) Headquarters (NSHQ) had in their ability to develop and maintain shared awareness and understanding with all their mission partner nations. [s, t, u, v]

Conclusion

Protecting information within stand-alone systems with well-defined and static cybersecurity requirements is a relatively straightforward task. Managing and satisfying cybersecurity requirements becomes increasingly difficult as environments (not only Multi-Domain C2 operational environments but also the R&D environments enabling them) become more complex with multiple inter-related and inter-dependent partners (Joint, Interagency, Multinational, and Public organizations). In these environments, C2 and C2-enabling system technical, operational and policy controls both affect, and are affected by the other systems.

In this paper we provided an update on our team's ongoing, cybersecurity-specific, positively disruptive, C2-enabling R&D efforts ((1) Quantum resistant, PSK-based CSfC cryptography, (2) Cross Classification Domain / Releasability Boundary (CD/RB) Solutions (CCSs), and (3) C2 Agility & Approaches Enabling Dynamic Security Control Sets and Overlays). We described the [Multiple classification and releasability, Alignment, Synchronization and Integration, Platform as a Service (MAPaaS) environment, to include citing inhibitors we encountered in developing the MAPaaS environment. We described the ASIF and Methodology that has been implemented to address the inhibitors encountered and to manage the MAPaaS and resulting cybersecurity RDT&E and Learning Environment. It is our expectation that, in 24th ICCRTS, our team will be able to provide an update on our C2-enabling cybersecurity R&D efforts along with updates and lessons learned from implementing ASIF and Methodology Stage 3 (Common Understanding) and Stage 4 (Coordination of Efforts & Common Measures of Progress).

REFERENCES

[a] 22nd ICCRTS "Pre-Shared Key-Enabled CSfC: A Positively Disruptive Technology and Enabler for Next Generation Mission Partner Secure Communications" Paper 026 6 Nov 2017

[b] Commercial Solutions for Classified (CSfC) FREQUENTLY ASKED QUESTIONS (Non-technical) Last Update: August 2015

[c] US NSA IAD Commercial Solutions for Classified (CSfC) Trifold 27 January 2017

[d] US NSA Central Security Service (CSS) Website: CSfC Approved Components List https://www.US NSA.gov/resources/everyone/csfc/components-list/

[e] US NSA Central Security Service (CSS) Website: CSfC Program https://www.US NSA.gov/resources/everyone/csfc/

[f] US NSA Central Security Service (CSS) Website: CSfC Capability Packages https://www.US NSA.gov/resources/everyone/csfc/capability-packages/

[g] Trident Warrior 2008 (TW08) Industry Day MCSBEN Poster board with Notes Guerin, 2008

[h] ONR Website: Mobile Secure Architecture http://www.onr.navy.mil/en/Media-Center/Fact-Sheets/Mobile-Architecture-Security.aspx

[i] US NSA Website: Overview of US NSA Suite B Ciphers http://www.US NSA.gov/ia/industry/cep.cfm

[j] National Institute of Standards and Technology Internal Report (NISTIR) 8105 Report on Post-Quantum Cryptography April 2016

[k] US NSA IA Directorate website: "Commercial National Security Algorithm Suite" page https://www.iad.gov/iad/programs/iad-initiatives/cUS NSA-suite.cfm

[l] Commercial National Security Algorithm (CUS NSA) Suite Factsheet 12/30/2015 **Identifier:** MFS-U-OO-814670-15

[m] US NSA Information Assurance Directorate (IAD) National Security Algorithm Suite and Quantum Computing FAQ MFQ U/OO/81099-15 January 2016

[n] Department of Defense Instruction (DoDI) 8510.01 Risk Management Framework (RMF) for DoD Information Technology (IT) March 12, 2014 (Incorporating Change 2, July 28, 2017) http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001_2014.pdf

[o] NATO SAS-085 C2 Agility Final Report, NATO STO-TR-SAS-085, 2013

[p] DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle September 2015 Version 1.0 http://www.acqnotes.com/wp-content/uploads/2014/09/PM-Guidebook-for-Integrating-Cybersecurity-RMF-into-System-Acquisition-Lifecycle-Sep-2015.pdf

[q] Use of Security Overlays or Control Sets in Addressing Control Deviations for Mortar Systems 27 April 2016 Mr. Daniel F. Campbell – U.S. Army ARDEC, Picatinny Arsenal

[r] NATO Network Enables Capability (NEC) Command & Control (C2) Maturity Model http://www.dodccrp.org/files/N2C2M2web_web_optimized.pdf

[s] ASIF Methodology http://www.asif-methodologies.com/

[t] 19th ICCRTS "A Methodology to Improving Unity of Effort for Mission Partner Planning" Paper 003 17 June 2014

[u] 21st ICCRTS "Improving Alignment and Unity of Effort with Mission Partners" Paper 001 6 September 2016

[v] 22nd ICCRTS "Improving C2 Alignment and Integration" Paper 004 6 November 2017

[w] 22nd ICCRTS "Improving Cyber Security Alignment and Integration" Paper 005 6 November 2017