OUTCOME 4

UNDERSTANDING INTER-DOMAIN DEPENDENCIES & VULNERABILITIES

CONCEPTUAL AND PRE-DOCTRINAL PAPER

31 JANUARY 2013

U.S.-CREST

FONDATION pour la RECHERCHE STRATÉGIQUE

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **08 JUL 2013**	2. REPORT TYPE **N/A**	3. DATES COVERED

4. TITLE AND SUBTITLE **Multinational Experiment 7 OUTCOME 4 UNDERSTANDING INTER-DOMAIN DEPENDENCIES & VULNERABILITIES CONCEPTUAL AND PRE-DOCTRINAL PAPER 31 JANUARY 2013**	5a. CONTRACT NUMBER 5b. GRANT NUMBER 5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER 5e. TASK NUMBER 5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **JOINT STAFF-MN//ACT Integration 116 Lakeview Parkway Suffolk, VA 23435**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S) 11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES

The original document contains color images.

14. ABSTRACT

This document aims to capture some of the conceptual and pre-doctrinal considerations developed in the context of MNE 7 Outcome 4 related to Inter-Domain Understanding. Although the focus of MNE 7 Outcome 4 was on the development of a methodology to identify inter-domain dependencies and related vulnerabilities, a number of broader considerations emerged in support of this methodology. They are encapsulated here. It is important to note that unless specified, the considerations described in this paper have not been subject to experimentation during MNE 7.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**UU**	**54**	

DISTRUBUTION STATEMENT

This document was developed and written by the contributing nations and organizations of the Multinational Experiment (MNE) 7. It does not necessarily reflect the views or opinions of any single nation or organization, but is intended as a guide. Reproduction of this document and unlimited distribution of copies is authorized for personal and non-commercial use only. The use of this work for commercial purposes is prohibited; its translation into other languages and adaptation/modification requires prior written permission. Questions or comments can be referred to MNE7_secretariat@apan.org

Table of Contents

Table of Abbreviations

A2/AD	Anti-Access and Area Denial
BLOS	Beyond Line of Sight
BMS	Ballistic Missile Defense
C2	Command and Control
CAOC	Combined Air and Space Operations Center
CC	Critical Capability
CCJO	Capstone Concept for Joint Operations
CIMIC	Civil-Military Co-Operation
CJTF	Combined Joint Task Force
CNO	Computer Network Operation
COA	Courses of Action
CoG	Center of Gravity
COM	Communications
CR	Critical Requirement
CV	Critical Vulnerability
DOTMLPFI	Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Interoperability
ECOA	Enemy Courses of Action
EHF	Extremely High Frequency
ELINT	Electronic Intelligence
eLORAN	Enhanced Long Range Navigation
FoN	Freedom of Navigation
GBS	Global Broadcast Service
GEOINT	Geo-Intelligence
GPS	Global Positioning System
HALE	High Altitude Long Endurance
HQ	Headquarters
HUMINT	Human Intelligence
IADS	Integrated Air Defense Systems
ID	Inter-Domain
ID-BAR	Inter-Domain Baseline Assessment Report
IDWG	Inter-Domain Working Group
IMINT	Imagery Intelligence
ISR	Intelligence, Surveillance, and Reconnaissance
J2	Joint Intelligence
JFHQ	Joint Force Headquarters

JOA	Joint Operations Area
JOAC	Joint Operational Access Concept
JPG	Joint Planning Group
KD	Knowledge Development
Kmap	Knowledge Map
LCC	Land Component Commander
LORAN	Long Range Navigation
LOS	Line of Sight
MALE	Medium Altitude Long Endurance
MASINT	Measurement and Signature Intelligence
MET	Mission Essential Task
MILSATCOM	Military Satellite Communications
MNE 7	Multinational Experiment 7
MOC	Maritime Operations Center
NEO	Non-Combatant Evacuation Operations
OC	Outcome
OCA	Offensive Counter-Air
PMESII	Political, Military, Economic, Social, Information, and Infrastructure
PNT	Positioning, Navigation, and Timing
POE	Preparation of the Operational Environment
RADINT	Radar Intelligence (from Non-Imaging Radar)
RCC	Regional Combatant Command
RF	Radio Frequency
SA	Situational Awareness
SAR	Satellite Synthetic Aperture Radar
SATCOM	Satellite Communications
SEAD	Suppression of Enemy Air Defenses
SHF	Super High Frequency
SIGINT	Signals Intelligence
SLOC	Sea Line of Communication
SME	Subject Matter Expert
SOV	System Operational View
SPOD	Sea Ports of Debarkation
UAS	Unmanned Aircraft System
UHF	Ultra-High Frequency

Preamble

This document aims to capture some of the conceptual and pre-doctrinal considerations developed in the context of MNE 7 Outcome 4 related to Inter-Domain Understanding. Although the focus of MNE 7 Outcome 4 was on the development of a methodology to identify inter-domain dependencies and related vulnerabilities, a number of broader considerations emerged in support of this methodology. They are encapsulated here. It is important to note that unless specified, the considerations described in this paper have not been subject to experimentation during MNE 7.

Readers interested in this topic should also examine the Methodology to Understand Inter-Domain Dependencies and Vulnerabilities, Guide version 1.0, 31 January 2013.

Sponsored by the United States Joint Staff J7 Joint and Coalition Warfighting, Multinational Experiment 7 (MNE 7) was the latest campaign in a series that started in the early 2000s. MNE 7 focused on developing improved coalition concepts and capabilities to ensure access to and freedom of action within the Global Commons[1]. While the expression "Global Commons" and the strategic framework it encompasses are not fully recognized by all MNE 7 nations, this theme was chosen because it enabled the MNE 7 community to address many issues of concern that necessitate new solutions. These concerns pertain namely to trends such as the increase in cyber attacks or other technology-related trends, which, as noted in the NATO 2010 Strategic Concept, may impact military operations, as well economic activities by disrupting communication, transport and transit routes and thus require international efforts to address them and to increase resilience[2].

[1] In MNE 7, the Global Commons include portions of the maritime and air domains, as well as space and cyberspace, and are defined as "*Areas that are potentially accessible to any and all actors – be they states, non-state, or individuals. Although this term is generally applied only to those areas that are not under the jurisdiction of any nation, MNE 7 will address areas that fall under some degree of national sovereignty when they are relevant to ensuring access to and freedom of action within the global commons*." (MNE 7 Campaign Lexicon v0.6 Definition, drawn from the MNE 7 Campaign Plan). The MNE 7 Campaign Lexicon further defines the Maritime, Air and Space Domains, as well as Cyberspace.

[2] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, *Active Engagement, Modern Defence*, November 2010, pages 11-12: "Cyber attacks are becoming more frequent, more organized and more costly in the damage that they inflict on government administrations, businesses, economies and potentially also transportation and supply networks and other critical infrastructure [...] A number of significant technology-related trends – including the development of laser weapons, electronic warfare and technologies that impede access to space – appear poised to have major global effects that will impact on NATO military planning and operations".

MNE 7 was organized into several parallel lines of work called outcomes (OC), each with multiple objectives, products and activities. In addition to three strands of work regarding the maritime, space and cyber domains respectively, "inter-domain" (ID) understanding became a fourth topic of work (Outcome 4), focused on addressing the linkages among domains. **"Inter-domain"** (ID) is the adjective qualifying something which is related to two or more different domains, to include the land, maritime, air, space and cyberspace domains.

An Inter-Domain Baseline Assessment Report (ID-BAR) was developed at the beginning of the MNE 7 campaign. This report stated that the ability to act in one domain of the Global Commons increasingly requires simultaneous access to and freedom of action within the others, while also noting that the increasing scope and rapid evolution of domain inter-relationships have made them critical issues. The ID-BAR furthermore identified three gaps, the most relevant of which to Outcome 4 is: "Nations and organizations have insufficient methodologies for comprehensively identifying, assessing and mitigating their vulnerabilities to an adversary's intra- and inter-domain warfighting strategies and capabilities[3]."

Taking into account these considerations, the aim of MNE 7 Outcome 4 was to arrive at a dynamic understanding of inter-domain vulnerabilities and risks that accounts for domain interrelationships in order to ensure freedom of action in the Global Commons. It was divided into two closely related objectives, which were in fact addressed together:

- Objective 4.1: Develop a method to understand and describe ID relationships, operating conditions, and mutual dependencies,
- Objective 4.2: Develop methodologies to identify and assess ID vulnerabilities and associated risks.

Despite the initial focus on the Global Commons (defined as portions of the maritime and air domains, as well as the space and cyber domains) the work on inter-domain understanding in MNE 7 took a broader view of these challenges by including all of the above mentioned domains, as well as the land domain.

While the main focus of Outcome 4 was primarily on the development of a methodology that could supplement existing analysis and planning processes in order to take into account an inter-domain perspective, this work also required developing some broader considerations that could be utilized to raise awareness about this topic and potentially serve educational purposes. That is the aim of this publication.

[3] MNE 7 Inter-Domain Baseline Assessment Report, version 1.0, April 2011, page 29. Accessible at https://wss.apan.org/s/ME/MNE/BaseAssess/7ID/(U-NFPR)%20MNE%207%20-%20GC%20Inter-Domain%20BAR%20V1%200_%2020110411.docx

Indeed, this document begins by addressing the military problem related to inter-domain understanding. It then focuses on ways of building inter-domain understanding, through a conceptual framework and models as well as a related methodology[4]. It also addresses some potential implications related to developing this inter-domain understanding. Finally, it provides illustrative examples to bring to light some inter-domain aspects of two fictional operations.

***

[4] The methodology is summarized in this document. It is explained more fully in the MNE 7 Outcome 4 Methodology to Understand Inter-Domain Dependencies and Vulnerabilities, Guide version 1.0, 31 January 2013.

Intentionally Blank

Part 1: The Military Problem

The topic of "inter-domain understanding" first emerged in MNE 7 within the context of the Global Commons. However, as work on this topic progressed, it became clear that "inter-domain" did not solely concern the Global Commons but rather related to the entirety of each of the four domains comprising the Global Commons as well as the land domain. Therefore, the notion of what "inter-domain" should encompass was broadened to include the land domain, as it was apparent that a failure to do so would be a clear oversight. The following section explains the context of the work undertaken on inter-domain understanding, drawing from the existing body of literature on the topic.

1- The Global Commons and Inter-Domain Understanding

As explained in the preamble of this document, the expression "Global Commons" began appearing in American defense publications towards 2009. Soon thereafter, it seemed to quickly develop into a new framework for strategic thinking in various studies and strategic documents in 2010 and 2011 and appeared both in the *U.S. National Security Strategy* and the *Quadrennial Defense Review*, albeit framed somewhat differently. The NATO Strategic Concept, while avoiding the use of the expression "Global Commons", highlighted many themes often associated with this topic, such dependencies on vital communication, transportation and transit routes – particularly in the context of energy supplies and trade – and noted trends such as the increase in cyber attacks and the development of other technologies with potential anti-access implications[5]. The topic of the Global Commons was furthermore explicitly explored by Allied Command Transformation (ACT), which published its results in April 2011 in a report entitled "Assured Access to the Global Commons".

While there is no officially agreed definition of the Global Commons, there is a certain consensus surrounding the idea that they are areas or domains that fall outside the direct jurisdiction of sovereign states, but are of interest to all and can be used by anyone. According to the *U.S. National Security Strategy*, the Global Commons are "the connective tissue around our globe upon which all nations' security and prosperity depend[6].

[5] Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, Active Engagement, Modern Defence, November 2010, pages 11-12

[6] *U.S. National Security Strategy* (NSS), 2010, pages 49-50. Note that in the NSS, the cyber domain is not included in the Global Commons.

The literature on the Global Commons tends to emphasize the ideas that they are increasingly contested and that it is important to maintain freedom of access to them. A number of experts note that trends such as the emergence of new military powers pursuing high-end asymmetric capabilities and the dissemination of disruptive technologies (civilian, military and dual) to state and non-state actors may lead to an extension of anti-access capabilities and threaten freedom of action in the Commons[7]. There is a concern that over time, this could have implications on the international order, due to potential limitations on freedom of movement and trade as well as new difficulties for military force projection. The ACT "Assured Access to the Global Commons" report for example states that "in the coming decade the Alliance will face an adversary that will pose a range of threats to assured access and use by NATO across the four domains"[8].

Thus, freedom of access to the Global Commons remains of key importance from a strategic, economic and military point of view. The ACT report quoted above notes that a "large part of NATO's strength and success comes from its ability to use the Global Commons in accordance with international law"[9]. Yet, new complexities in the Global Commons may substantially and unexpectedly lessen military effectiveness: "[g]iven integrated and highly interdependent domain relationships, degrading one system in one domain has the potential to exponentially increase degradation in all other systems"[10]. Captain (USN) Redden and Colonel Hughes consider that "serious analytical attention has not been devoted to cross-domain issues such as these"[11]. They see "a clear need for more detailed analysis of the global commons, along with a systematic determination of domain interdependencies, identifying the resultant risks and rewards and the appropriate means of incorporating them into military strategy, concepts and doctrine"[12] and recommend that strategists and defense planners "depart from the domain-centric mindset and take a broader perspective when viewing the commons. They must employ a holistic approach that breaks down domain stovepipes and treats the global commons not as a set of distinct geographies, but rather as a complex, interactive system"[13].

[7] Abraham Denmark: "Managing the Global Commons"; *The Washington Quarterly*; July 2010, page 165.

[8] Mark Barrett, Dick Bedford, Elizabeth Skinner, Eva Vergles: *Assured Access to the Global Commons*, April 2011, page ix.

[9] Ibid, page xii. The report further notes that "[o]ver time, access has become paramount to our ability to move troops into far-flung theaters of operation, to maintain command and control through the use of advanced information technology in space and cyberspace, to control airspace in support of combat and rescue operations, and to support international disaster relief across the globe".

[10] Mark E. Redden and Michael Hughes: "Global Commons and Domain Interrelationships: Time for a New Conceptual Framework? *Strategic Forum number 259, Institute for National Strategic Studies (INSS), National Defense University,* October 2010; page 7. Captain Redden and Colonel Hughes' work was influential in framing the inter-domain aspects of the MNE 7 campaign.

[11] Ibid, page 7.

[12] Ibid, page 9.

[13] Ibid, page 8.

2- Inter-Domain Understanding beyond the Global Commons, with a Focus on Space and Cyber

In spite of having gained visibility in the context of the Global Commons, inter-domain understanding:

- Is relevant beyond the scope of issues related to the Global Commons;
- Should focus more specifically on the implications of cyber and space domains on joint operations at present and in the foreseeable context.

As seen above, understanding interactions among different domains is increasingly important for most engagements, whether or not the initial stake is necessarily linked to the access to, or control of, the Global Commons *per se*. As developed below, interactions created through space and cyber deserve a special consideration.

In line with the recognition of the importance of the inter-domain dimension of current and future engagements, U.S. publications have increasingly incorporated the notion of "cross-domain", often used in the context of "cross-domain synergy". This expression can be found particular in joint concepts, such as the Capstone Concept for Joint Operations (CCJO), the Joint Operational Access Concept (JOAC) or the Army-Marine Corps concept on gaining and maintaining access. It is interesting to note that the CCJO begins by framing the problem in terms of risk to access to the Global Commons but then broadens it to the ability to fight simultaneously across domains[14].

These various documents also highlight the importance of space and cyberspace, and the impact that degradations in these domains can have on operations[15].

Indeed, one may assume that the cross-domain synergy related strictly to the land, sea, and air operations is well addressed by the notion of jointness, which has been incorporated over the last several decades into doctrine, training and education programs and ultimately, mind-sets.

[14] Capstone Concept for Joint Operations: Joint Force 2020, 10 September 2012, page 2: "*The proliferation of cyber and space weapons, precision munitions, ballistic missiles, and anti-access and area denial capabilities will grant more adversaries the ability to inflict devastating losses. These threats place our access to the global commons at risk, target our forces as they deploy to the operational area, and can even threaten forces at their points of origin. Meanwhile, adversaries continue to explore asymmetric ways to employ both crude and advanced technology to exploit U.S. vulnerabilities. Consequently, the capability advantage that U.S. forces have had over many potential adversaries may narrow in the future. Adversaries will not only have more advanced capabilities in every domain. More of them will have the ability to simultaneously fight across multiple domains.*"

[15] Capstone Concept for Joint Operations: Joint Force 2020, 10 September 2012, pages 2-3.

The military problem we are confronted to is more specifically caused by the following trends:

- The increasing level of reliance of traditional joint or domain-specific operations on space and cyber related capabilities. This reliance is particularly critical when an engagement requires a strong level of interaction and synergy between the activities planned in the different traditional domains.

- The level of sophistication of the means available to potential hostile actors, particularly their ability to affect the cyber and space domains.

Dynamics such as the emergence of hybrid threats or the risk of conventional conflicts involving regional and emerging powers who are well-equipped with anti-access and other sophisticated assets will probably reinforce the criticality of inter-domain issues in future engagements.

Therefore, **the military problem is that the increasing vulnerability of coalition forces in and through the space and cyber dimensions may now hinder or threaten their ability to achieve their objectives.**

These trends make it important to better understand the implications of inter-domain dependencies, focused on the space and cyber domains implications, and the vulnerabilities that may stem from them. Inter-domain understanding can then inform planning, mitigation options and help to build resilience.

Part 2: Building Inter-Domain Understanding

An important step in arriving at a better understanding of inter-domain issues, focusing on the impact of dependencies on space and cyber space, as seen in the previous section, consists in a clarification of the related vocabulary and in a depiction of the main challenges associated with this topic. It requires a more systematic way of thinking about inter-domain relationships and the dependencies and vulnerabilities that may stem from them. The first step towards building inter-domain understanding is the development of a conceptual framework. Subsequent steps may involve efforts to model and analyze these relationships. A methodology can be a useful tool to that end.

1- Inter-Domain Conceptual Framework

This conceptual framework defines the key terms to be used to consider ID issues and explains the linkages between them. It can be used as a common reference for planners – at the strategic and operational levels – but also as a way to encourage thinking about inter-domain considerations more broadly[16]. It is based on the notion that there is an "Inter-Domain System", as defined here, for each engagement of a military force. The figure below provides a visualization of the key terms and the relationships between them[17]. They are then explained in the text below.

[16] This conceptual framework provides the intellectual underpinning of the methodology developed in MNE 7 Outcome 4: Methodology to Understand Inter-Domain Dependencies and Vulnerabilities, Guide version 1.0, 31 January 2013.

[17] They are organized as an ontology. The word ontology is used in this guide is the sense of a "formal specification of a shared conceptualization" as defined by Tom Gruber in, "What is an ontology": http://www-ksl.stanford.edu/kst/what-is-an-ontology.html, (accessed on 04 April 2012). An ontology is a semantic model (i.e. something related to the meaning of "concepts" or terms) that represents the knowledge about a given topic. The terms are linked by semantic relationships.

Typically, an ontology is composed of:

- CLASSES - The terms and their classification (taxonomy)
- RELATIONSHIPS – The way in which terms are connected or work together, as a semantic expression
- AXIOMS - The sentences stating true facts that can be built with terms and relationships, that contains the knowledge we have developed

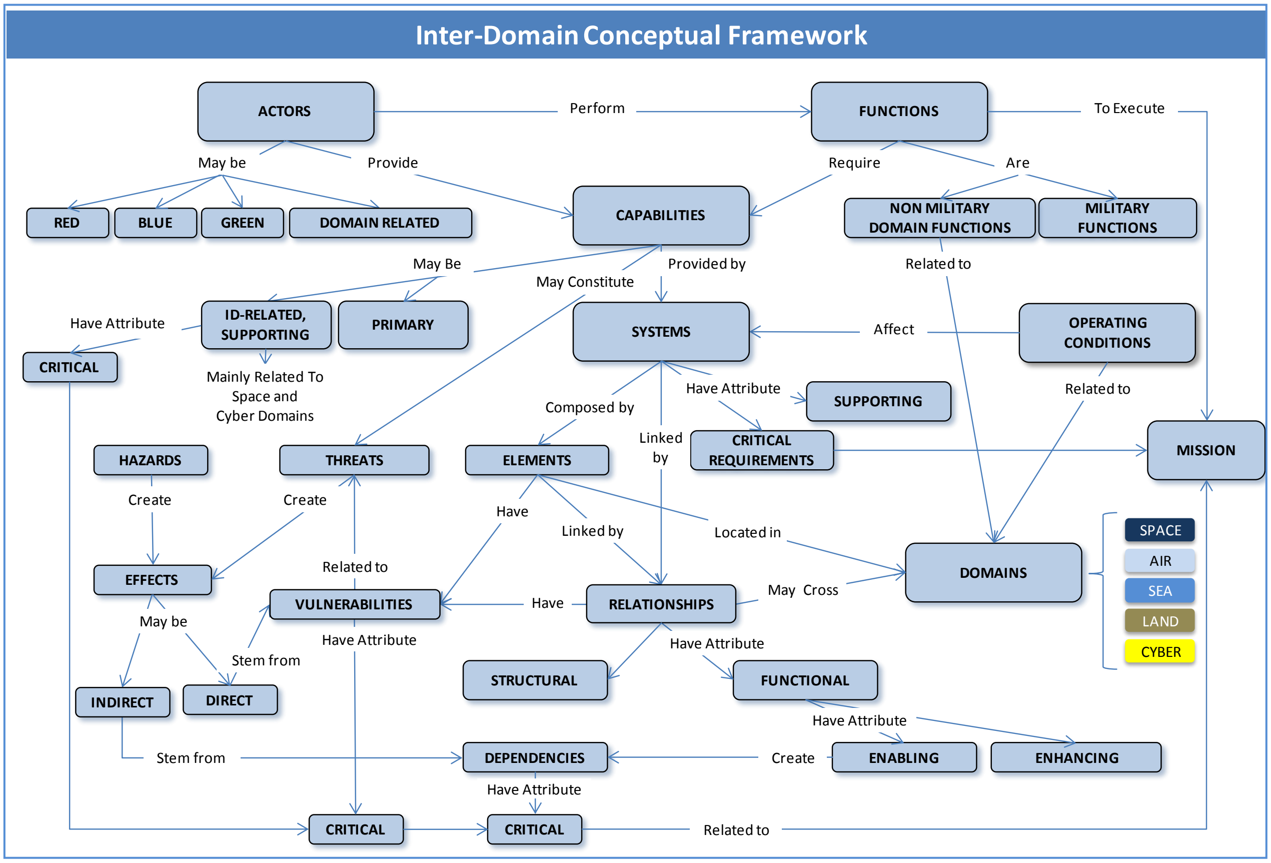

Figure 1: Inter-Domain (ID) Conceptual Framework

1.1 An Inter-Domain System

Each **domain** is characterized by a specific geographical and/or technical environment in which there are a variety of actors, systems or assets (e.g.: ships, aircraft, satellites), or other types of elements in cyberspace (hardware, software or data related).

"Inter-domain" is the adjective qualifying something which is related to two or more different domains (land, maritime, air, space, cyber).

An **"Inter-Domain System"** is the functionally, physically or behaviorally related group of elements forming a unified whole, which dynamically connects the different domains and allows the interactions between capabilities and activities of these domains. The perimeter of an inter-domain system, like that of any other complex system, is bounded by a given perspective and is context specific. Therefore, a specific Inter-Domain System can be identified for each engagement of a military force. While it is obvious that certain assets will be used regardless of the operation (e.g. the GPS system), many elements of an ID System will differ from one engagement to another. Thus, an "ID System" is relative in nature and in scope.

An ID System is composed of **elements**. An element of an ID System is a specific physical, functional or behavioral entity, which can be resident in one or more domains and may be a space, air, maritime, land or cyber asset. Depending on the level of granularity, an element may be itself decomposed as a system, which may be inter-domain. Many weapons systems are typically inter-domain, with components located in different domains (such has an unmanned aerial system, with airborne, ground based and cyber components); all space and cyber systems are inter-domain (space systems have space, land and cyber components, and cyber systems always have some physical components – such as computer hardware or communication links – located in one of more geographical domains).

1.2 Actors

All parties and stakeholders that are part of the operational environment and either directly or indirectly have a share, take part, or influence the outcome of an engagement.

Actors perform functions. They can have capabilities or can own systems or elements required for a capability.

The actors to be considered in an ID System include:

- The "Blue" force;
- The designated adversary or non-compliant actors opposing the mandate of the force ("Red");
- The "Green" actors, notably other state and non-state entities, in the area of interest;
- The civilian "domain-related actors" of the area whose activities in one domain have a strong inter-domain dimension. They operate in and/or regulate the various domains and can be a sub-set of the previous categories.

1.3 Functions and Capabilities

A distinction is made here between Military Functions, which are also referred to as "Joint Functions" in U.S. doctrine, and what are called "Non-Military Domain Functions", which is a new term, created for the purpose of inter-domain analysis. One way of looking at inter-domain relationships is to categorize them by function as done in the "functional models" described in the next section.

1.3.1 Military Functions

Military Functions are the related capabilities and activities grouped together to help joint force commanders synchronize, integrate, and direct joint operations[18]. According to NATO and U.S. doctrine, these Military Functions are:

- Command and control,
- Intelligence,
- Fires (lethal and non-lethal),
- Movement and Maneuver,
- Protection,
- Sustainment.

Military Functions may be “Blue”, “Red” or “Green”.

1.3.2 Non-Military Domain Functions

“Non-Military Domain Function” is a term developed in MNE 7 and used in the MNE 7 Outcome 4 Methodology to Understand Inter-Domain Dependencies and Vulnerabilities (Guide version 1.0, 31 January 2013). Indeed, while Military Functions are useful to understand, and possibly map and analyze inter-domain dependencies and vulnerabilities in the military sphere, inter-domain issues also concern the civilian sphere. Thus, the term “non-military domain function” is used to refer to the non-military activities and capabilities that take place in the domains as related to an area of interest. These activities include primarily access to and operations within (transit and resources exploitation) each domain. They may be decomposed into various “value chains”[19]. For example, for the space domain, activities may be related to space system manufacturing, launch of space assets, fleet operations and maintenance and provision of services.

1.3.3 Capabilities

A **capability** can be defined as the output that can be delivered by a combination of Doctrine, Organization, Training, Materiel, Leadership development, Personnel, Facilities and Interoperability (DOTMLPFI) resources.

Most capabilities have an inter-domain dimension because they are provided by systems or assets that have elements in more than one domain, or enable or affect a capability in

[18] US Joint Publication 3-0, *Joint Operations*, 11 August 2011, p III-1, definition of “joint function”

[19] Porter’s Values Chain model is used to understand the activities of the business sector, which consider for a given firm several chains of activities: “inbound logistics”, Operations, “Outbound logistics”, Marketing and sales, and Service. These chains are supported by Infrastructure, Technology Development, Human Resource Management, Procurement. See: http://www.netmba.com/strategy/value-chain/

another domain. Each domain hosts systems and assets, that are either themselves inter-domain or provide capabilities that have a strong ID dimension. *For example:*

- *Logistics capabilities have an ID dimension because they rely on seaports or airports, which are inter-domain assets.*
- *Counter-land capabilities have an ID dimension because they are provided by strike assets in the maritime and air domains.*

Given that the traditional interactions among land, maritime and air domain activities are already well taken into account through the concept of jointness, in light of the military problem described in part 1, it is most useful to focus on the implications of activities in the space and cyber dimensions. Doing so should help to address the gaps related to operational-level staffs' understanding of dependencies and vulnerabilities related to the cyber and space domains, as well as to the low degree of integration of their related activities with other operational issues.

In order to focus on the implications of cyber and space domains, a distinction is made here between:

- **Primary capabilities**, which are capabilities that directly ensure a specific military function (e.g. collection capabilities for the intelligence function, interdiction for the fires function);
- **ID-related supporting capabilities**, which are capabilities that enable the primary capabilities and are not specific to a military function. (e.g. PNT capabilities supporting collection capabilities for the intelligence function) and are mainly (but not exclusively) provided by space and cyber systems.[20]

The basic ID related supporting capabilities are:

- Communications, which may be decomposed into:
  - BLOS (Beyond Line of Sight) capabilities provided notably by SATCOM systems but also by radio systems
  - Line of Sight (LOS) capabilities typically provided by data links
  - Wired Communications capabilities
- Positioning, Navigation and Timing (PNT)
- Information Management provided mainly by the logical layer of the cyber domain (including data, protocols and applications)

[20] Note that the expression "primary" vs. "ID-related supporting" are specific to this document and to the work done in MNE 7. Primary capabilities are drawn from the Joint Capability Areas developed by the U.S. Departement of Defense.

- Remote Sensing, which is supported by the three above-listed capabilities. It can potentially be provided by sensor systems operating not only in space but also in other physical domains.

Please refer to appendix A for a list of ID-related capabilities from each domain's perspective.

The intent of this distinction between "primary" vs. "ID-related supporting" capabilities is to facilitate the development of a comprehensive view of the capabilities required to execute a mission. Note that the "primary" or "ID-related supporting" nature of a capability may differ according the circumstances, the considered systems and doctrine. It may not encompass all the systems of a given capability. This is notably the case for information management and remote sensing. *For example, "remote sensing" systems should be considered primary capabilities when they are exclusively part of the collection assets of the Intelligence function; remote-sensing systems should be considered ID-related supporting capabilities when they provide combat information to Command and Control, Fires or Protection.*

ID-related supporting capabilities may also be deemed critical when they are essential to the accomplishment of the specified or assumed objective(s).

1.4 Operating Conditions

Operating conditions are the conditions of each engagement which stem from the operational environment and other mission-related factors, such as the constraints and restraints. They may determine and/or affect the ID System, its system elements and relationships.

1.5 Relationships, Dependencies and Vulnerabilities

An ID System is characterized by the dependencies between its elements and related capabilities, as well as by vulnerabilities and associated risks created by hazards and threats. Relationships are not necessarily specific to an ID System and some of them may be standing. However, it is necessary to understand the relationships in order to then identify dependencies.

1.5.1 ID Relationships

Inter-domain relationships can be defined as the connection between two elements of an ID System. They may be structural, functional or behavioral. It is useful to distinguish between enabling and enhancing relationships:

- An enabling relationship is a functional relationship through which an element, system, or operating condition makes feasible or possible the ability of another element to accomplish its expected task as intended.
- An enhancing relationship is a functional relationship through which an element, system, or operating condition improves the ability of another element to accomplish its expected task as intended.

1.5.2 ID Dependencies

An **inter-domain dependency is** the state, for a system element, of being solely reliant for support on another system element located in another domain.

Dependency is related to a specific context and is relative to a technical, operational or functional need. From a functional perspective, the dependency of an element stems from a **single enabling relationship** for which there is no alternative. By extension, the term "ID dependency" can be used to designate the element which provides this single enabling relationship.

A **critical inter-domain dependency** is an inter-domain dependency which is essential to the achievement of the mission.

A critical inter-domain dependency may cover the following situations:

- When the dependency is essential to the accomplishment of the mission (i.e. the dependency of a CoG critical requirement);
- When a large number of systems needed to fulfill a given military function depend on the same enabler, the failure of which would have an adverse cumulative impact on the accomplishment of the mission.

For example, GPS is considered to be a critical dependency because of its single enabling relationship (for which there is no alternative) with attack aircraft to conduct precision strikes with a certain type of munitions, which in turn represents a critical requirement to perform offensive air operations.

1.5.3 Threats

A **threat** is defined as the combination of implied or expressed intentions, capabilities, and willingness of one actor to negatively affect another actor and its assets.

1.5.4 Hazards

A **hazard** is defined as an actual or potential non-hostile action or condition which may cause a negative effect on an element or a relationship of the ID System.

1.5.5 Vulnerabilities

Vulnerabilities are the characteristics of a system that render it open to exploitation or susceptible to a given hazard or threat, possibly resulting in an impaired capability to perform a designated task.

A **critical inter-domain vulnerability** is the vulnerability of a system that constitutes a critical ID dependency (due to the fact that it is essential to the achievement of the mission). By extension, the term "critical ID vulnerability" can be used to designate the system itself.

1.6 Dynamic Perspectives

An ID System is dynamic in nature. Several points are important to consider:

- An ID System will be characterized by chains of enabling relationships between its elements. These chains multiply the risk that:
  - Indirect approaches by an adversary can affect the critical dependencies of this ID System;
  - A specific action or hazard will cause various indirect effects on these critical dependencies, and ultimately on capabilities and functions, due to the propagation of these effects along the above-mentioned chains of enabling relationships;
- It is also important to consider that, given the different characteristics of each domain, these chains of effects may have heterogeneous timeframes, ranging from seconds for activities in the cyber domain to weeks for activities in the maritime domain;
- Finally, the ID System, as well as its interactions with actors and operating conditions, varies dynamically according to the evolving nature of the engagement. The increasing importance of an operating condition throughout the engagement may lead to changes relating to the force's critical ID dependencies and vulnerabilities.

***

2- Inter-Domain Functional Models

2.1 Introduction

2.1.1 Purpose

The purpose of the ID functional models is to provide an overall perspective of the possible inter-domain relationships between capabilities related to the different military functions or non-military domain functions. The ID functional models are generic, reflecting the fact that a number of standing inter-domain relationships between systems and elements remain unchanged regardless of the context; they are not related to a specific set of capabilities or to a specific situation.

They can be used during planning as an intellectual tool to facilitate the identification and categorization of capabilities and systems, and their related inter-domain relationships, for a given military function or non-military domain function.

2.1.2 Content

ID functional models are based on a representation of the capabilities related to military functions or non-military domain functions, focusing on the implication of space and cyber capabilities. The representation also includes the systems and system elements [or sub systems] that contribute to a given capability as well as the ID relationships that functionally link these systems and sub systems together.

They include:

- A graphical depiction of the linkages among functions, primary and supporting capabilities, and related systems;
- A narrative providing a short explanation of the types and characteristics of inter-domain relationships that could exist among capabilities or activities to perform the given military function or a non-military domain function.

Ideally, an ID functional model would be developed in advance for:

- Each military function:
    - Command and control
    - Intelligence
    - Fires
    - Movement and maneuver
    - Force protection
    - Sustainment

- The non-military domain functions:
  - Maritime domain access and operations
  - Air domain access and operations
  - Space domain access and operations
  - Cyber domain access and operations.

Having these functional models can help to focus thinking on inter-domain relationships in relation to specific capabilities and functions. This understanding can in turn facilitate the mapping of inter-domain dependencies and the analysis of vulnerabilities for a specific operation.

2.2 Example of an Inter-Domain Functional Model: Intelligence Function

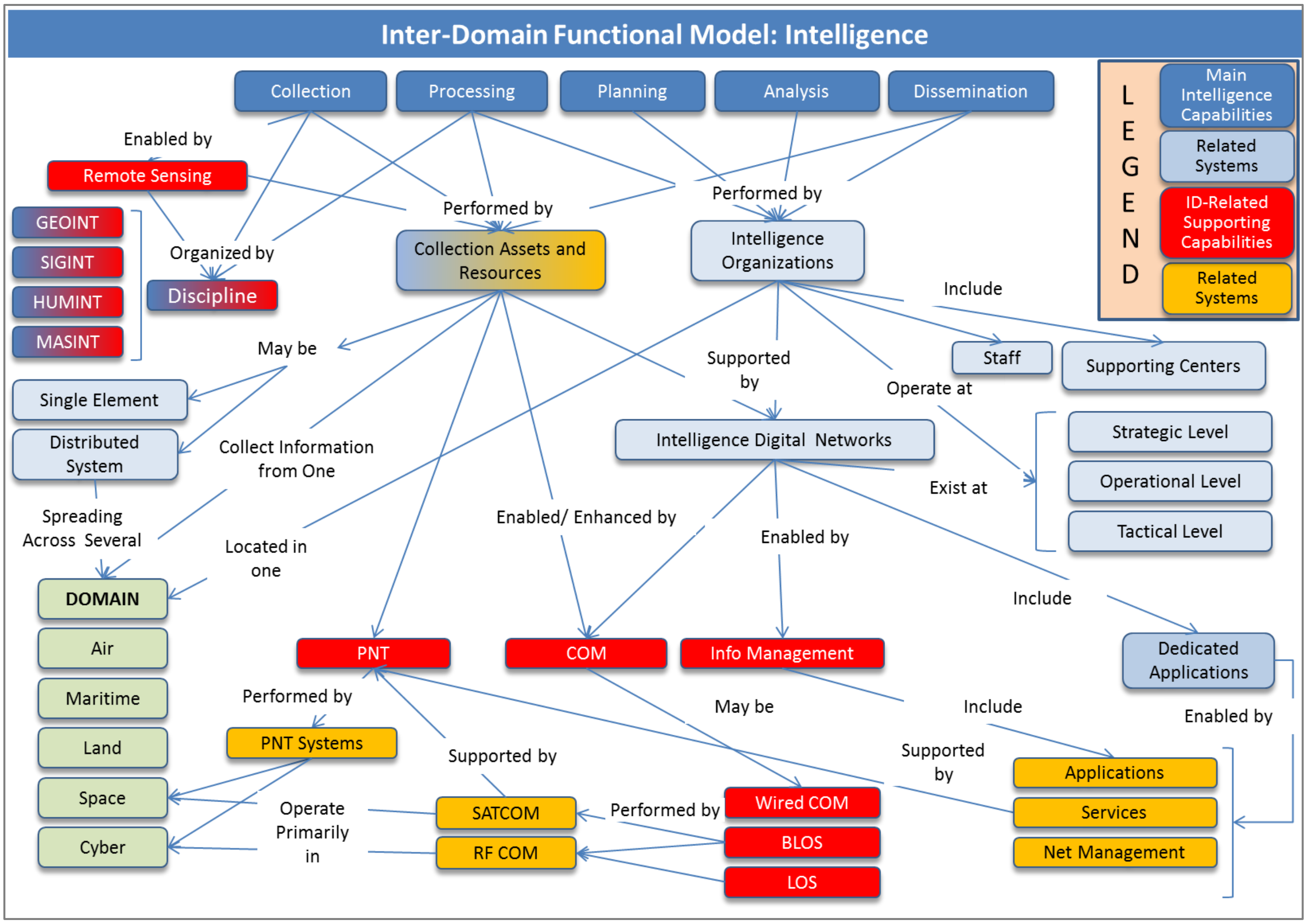

Figure 2: Representation of an Intelligence Functional Model

2.2.1 Introduction

This ID functional model, based on the ID conceptual framework described in the previous section, exposes the inter-domain dimension of capabilities enabling the intelligence function of a military force.

This model is articulated along several categories:

- The main capabilities needed for the intelligence function and the systems related to these primary capabilities;
- The ID-related supporting capabilities and the systems related to these ID-related supporting capabilities.

It focuses on the capabilities provided by systems operating primarily in the cyber and space domains.

2.2.2 Main Intelligence Capabilities and Related Systems

For the intelligence function, the main capabilities are the sub-functions of the intelligence process:

- Planning,
- Collection,
- Processing,
- Analysis
- Dissemination.

These primary capabilities, which in this case include "remote sensing" capabilities, are provided by the following systems and assets:

- <u>The intelligence organizations</u> have the following characteristics:
    - They include staffs and supporting processing and analysis centers,
    - They may
        - Plan intelligence and collection requirements
        - Process and disseminate intelligence in one or more disciplines:
            - Geo- intelligence (GEOINT)
            - Signals Intelligence (SIGINT)
            - Measurement and Signature Intelligence (MASINT)
            - Human Intelligence (HUMINT)
        - analyze and disseminate all-source intelligence products and
    - They may operate at the strategic, operational and tactical level, and
    - They may be located in different domains.
- <u>The collection assets and resources</u>, have the following characteristics:

  - They collect information primarily from one domain,
  - They are composed either of a single sensor element (for example a ship), or of an inter-domain system distributed in different domains (UAS for example),
  - They collect information in one or more disciplines:
    - Geo- intelligence (GEOINT)
    - Signals Intelligence (SIGINT)
    - Measurement and Signature Intelligence (MASINT)
    - Human Intelligence (HUMINT)
  - They include
    - The force's collection assets and other collection resources which are dedicated to the intelligence function or
    - Other collection resources of the force which are non-dedicated to the intelligence function.

- The intelligence networks that connect and support the intelligence organizations and the collection assets and may exist at the strategic, operational and tactical level. The intelligence networks include dedicated sets of applications.

2.2.3 ID-Related Supporting Capabilities, Related Systems and their Relationships

The intelligence networks and ISR systems are enabled by three ID-related supporting capabilities: information management capabilities, communications capabilities and PNT capabilities. These capabilities and supporting systems are described below.

- **The Intelligence networks** are enabled by:

  - Information management capabilities in the cyber domain, which include
    - the set of functional applications,
    - network management,
    - the provision of enterprise services, and
    - information assurance;
  - Communications capabilities, including
    - Switching and routing capabilities,
    - Wired-communications capabilities for long haul information transport between fixed intelligence organizations and with fixed elements of collection systems;
    - beyond Line of Sight (BLOS) communications, mainly provided by SATCOM systems
      - EHF/Ka Band secure SATCOM systems for secured, jam-resistant, low to medium data rate communications;
      - SHF/Ku Band SATCOM, either military and civilian, medium to high data rate, to broadcast GEOINT product;

            - UHF/S-Band/C-Band SATCOM for low data rate communications with mobile systems
        - Line of Sight (LOS) communications provided by other UHF RF communications;
    - PNT capabilities which enable the enterprise services of the network;

- **The airborne collection assets and resources** are enabled/enhanced by

    - Information management capabilities,
    - Communications capabilities allowing the transmission of C2 data of the collection system and collected data,
        - between the elements of the system (platform and control element)
        - between the system and intelligence organizations, such as processing centers and intelligence staffs

GEOINT and video transmissions are the most demanding in terms of bandwidth and require use of SHF Ku-Band. The communications capabilities include

        - Wired-communication capabilities between fixed elements of collection system
        - Beyond Line of Sight capabilities, the SATCOM systems
        - Line of sight capabilities, by other RF COM systems
    - PNT capabilities necessary for the positioning, navigation, and timing synchronization, which may be provided by:
        - The space PNT mainly provided by GPS[21],
        - Radio systems enabling positioning and navigation, notably the LORAN and eLORAN systems.

- **The naval collection assets and resources** are enabled/enhanced by:

    - Communications capabilities allowing the transmission of C2 data of the collection system and collected ISR data between the naval platform and users. Imagery and video transmissions are the most demanding in terms of bandwidth and require use of SHF Ku-Band. In the case of naval collection systems, these capabilities (mainly beyond Line of sight) are provided by the SATCOM.
    - PNT capabilities necessary for the positioning, the navigation, for the timing synchronization, which may be provided by:
        - The space PNT mainly provided by GPS[22],
        - The PNT radio, notably the LORAN and eLORAN systems.

[21] In the future it may also be provided by Galileo, GLONASS or BEIDOU.

[22] In the future it may also be provided by Galileo, GLONASS or BEIDOU.

- **The space-based collection assets and resources** are enabled/enhanced by:

  - Wired-communications capabilities between elements of the control segment of the system,
  - PNT capabilities that are necessary to control the spacecraft as well as their related communication links, and may be provided by space PNT systems.

ISR assets and resources provide both the intelligence function's collection capability and the bulk of remote sensing, which is considered here to be an ID-related supporting capability. Although most surveillance and reconnaissance systems were once primarily intended to feed intelligence analysis (as collection assets and resources), in network enabled operations they are also providing remote sensing capability in direct support of the C2, Fires and Protection functions. However, given that these ISR assets and resources are discussed in the context of the collection capabilities of the intelligence function, to avoid repetition they are not addressed a second time specifically with regard to remote sensing. Nevertheless, some ISR collection resources are not related to remote sensing (for example, all direct observation means), and some remote sensing assets are not intelligence-related even though the information they acquired could be exploited later for intelligence purposes. The latter include but are not limited to:

- Early warning systems;
- Battle management systems (providing RADINT/ Ground Moving Target Indications or Full-Motion Video);
- Weapon systems sensors (dubbed as "non-traditional ISR");
- Weather systems.

***

3- Developing a Methodology

Developing inter-domain understanding and incorporating it into planning requires a more systematic way of thinking about these issues. While the first step to improving inter-domain understanding is simply to think about these issues and to consider their potential impact on an operation, it is difficult to identify inter-domain vulnerabilities in an *ad hoc* manner, without the appropriate expertise and without a methodology to help identify the critical pieces.

Inter-domain vulnerabilities can be looked at from different perspectives:

- The identification of one's own (friendly) inter-domain vulnerabilities, usually for the purposes of protection and risk mitigation;
- The identification of an adversary's inter-domain vulnerabilities, potentially for targeting purposes;
- The identification of "Green" actors' inter-domain vulnerabilities.

While it is possible to think about inter-domain relationships in a generic manner, many of the dependencies and vulnerabilities that stem from them are context-specific. A methodology is therefore a useful way of identifying ID vulnerabilities.

3.1 Methodological Modules of the MNE 7 Outcome 4 Methodology

One such methodology, developed in MNE 7 Outcome 4, is built around of three iterative “modules” and focuses primarily on the identification of one’s own inter-domain vulnerabilities[23]. It draws on the inter-domain conceptual framework and functional models described in this chapter. The modules complement the early stages of the operational planning process. By framing the inter-domain aspects of an engagement (module 1), and analyzing inter-domain dependencies (module 2), it becomes possible to identify inter-domain vulnerabilities (module 3), which can enrich center of gravity analysis and contribute to mission analysis and course of action development. The three modules can be further described in the following manner:

1. **Module 1: Framing the inter-domain dimension of an engagement**. This module aims to identify the inter-domain issues in the engagement space, as well as the military functions, the non-military domain functions, and the capabilities to be taken into account in order to orient the subsequent steps of the methodology. It is an integral part of the problem framing undertaken at the beginning of the operational planning process.

2. **Module 2: ID relationships mapping and ID dependencies analysis.** The aim of this module is to map the relationships between the elements of the ID System and to understand the critical inter-domain dependencies. The level of detail at which

[23] Portions of the methodology (modules 2 and 3) as described in a version 0.8 of this guide were experimented during a limited objective experiment (LOE) in June 2012.
While participants in the LOE were generally satisfied with the methodology as they applied it and with the results they obtained, the LOE did not enable a complete investigation or “validation” of all of the methodology’s steps and sub-steps.
Practitioners composing the experiment audience stated that in their view, the methodology provided:

- A workable way to detect the vulnerabilities of blue forces’ inter-domain capabilities;
- Added value and fills a gap in existing analysis and planning processes in terms of ID issues.

However, despite this positive feedback, participants did not consider that the methodology had reached its full maturity and proposed a number of changes, mainly pertaining to its clarification. Recommendations stemming from the LOE are reflected the version 1.0 of the guide.
Some additional general findings from the LOE are:

- The guide provides a common framework to analyze and work with ID considerations for the different actors involved in the preparation of an operation.
- Cyber and space expertise is essential in order to implement the methodology.

the mapping and analysis is performed depends heavily on the time available to develop the preparation of the operational environment (POE) and on information available regarding the Blue and Green capabilities and resources.

3. **Module 3: Critical inter-domain vulnerabilities identification**. This module focuses on the analysis and correlation of the direct and indirect effects that would result from an attack or a hazard on vulnerable systems representing critical ID dependencies. This leads to the identification of the critical ID vulnerabilities.

The figure below provides a more detailed look at the key steps of each module.

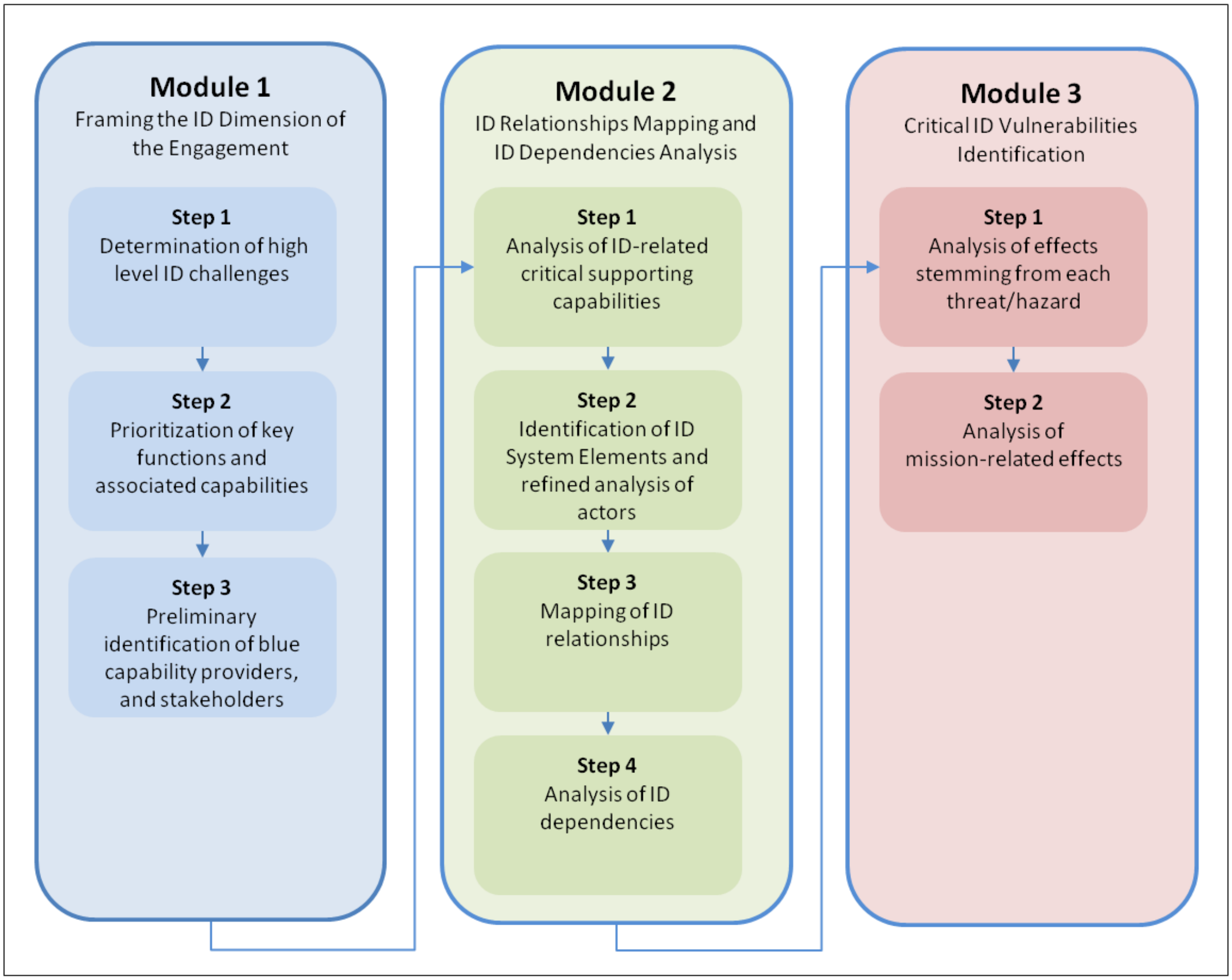
Module 1
Framing the ID Dimension of the Engagement
Step 1
Determination of high level ID challenges
Step 2
Prioritization of key functions and associated capabilities
Step 3
Preliminary identification of blue capability providers, and stakeholders
Module 2
ID Relationships Mapping and ID Dependencies Analysis
Step 1
Analysis of ID-related critical supporting capabilities
Step 2
Identification of ID System Elements and refined analysis of actors
Step 3
Mapping of ID relationships
Step 4
Analysis of ID dependencies
Module 3
Critical ID Vulnerabilities Identification
Step 1
Analysis of effects stemming from each threat/hazard
Step 2
Analysis of mission-related effects

Figure 3: Step-by-Step View of the Modules

These modules and their interactions with the decision-making processes may be visualized as follows:

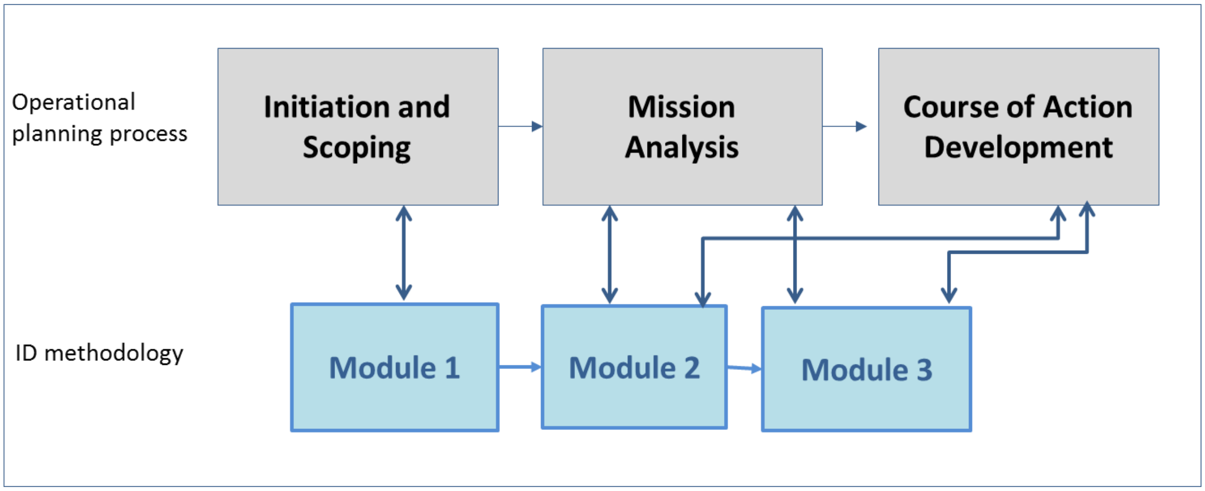

Figure 4: ID Methodological Modules in Relation to the Operational Planning Process

Modules 2 and 3 should be applied at two stages of the operational planning process:

- First, during mission analysis to contribute to a cross-functional analysis of the center of gravity. This work complements the analysis of the CoG critical capabilities, critical requirements and critical vulnerabilities.
- Second, in support of course of action development, drawing predominantly on the Enemy CoAs developed through the POE process and the initial COAs developed by the joint planning group. It consists of an update of the critical dependencies and vulnerabilities for these different CoAs based on the dynamics of the engagement. This analysis then feeds the development of the most dangerous ECoA, the risk analysis for the Blue COAs and the development of risk mitigation options.

The methodology may be implemented during standing strategic awareness, but is primarily designed to support contingency planning and crisis response planning within existing knowledge development/intelligence and operational planning processes.

3.2 Linkages between the Methodology and the Conceptual Framework

The methodology draws heavily on the conceptual framework, which provides its intellectual underpinnings. The two figures below represent “conceptual views” for modules 2 and 3 of the methodology. They show the logical linkages between notions developed in the conceptual framework as related to each of the modules.

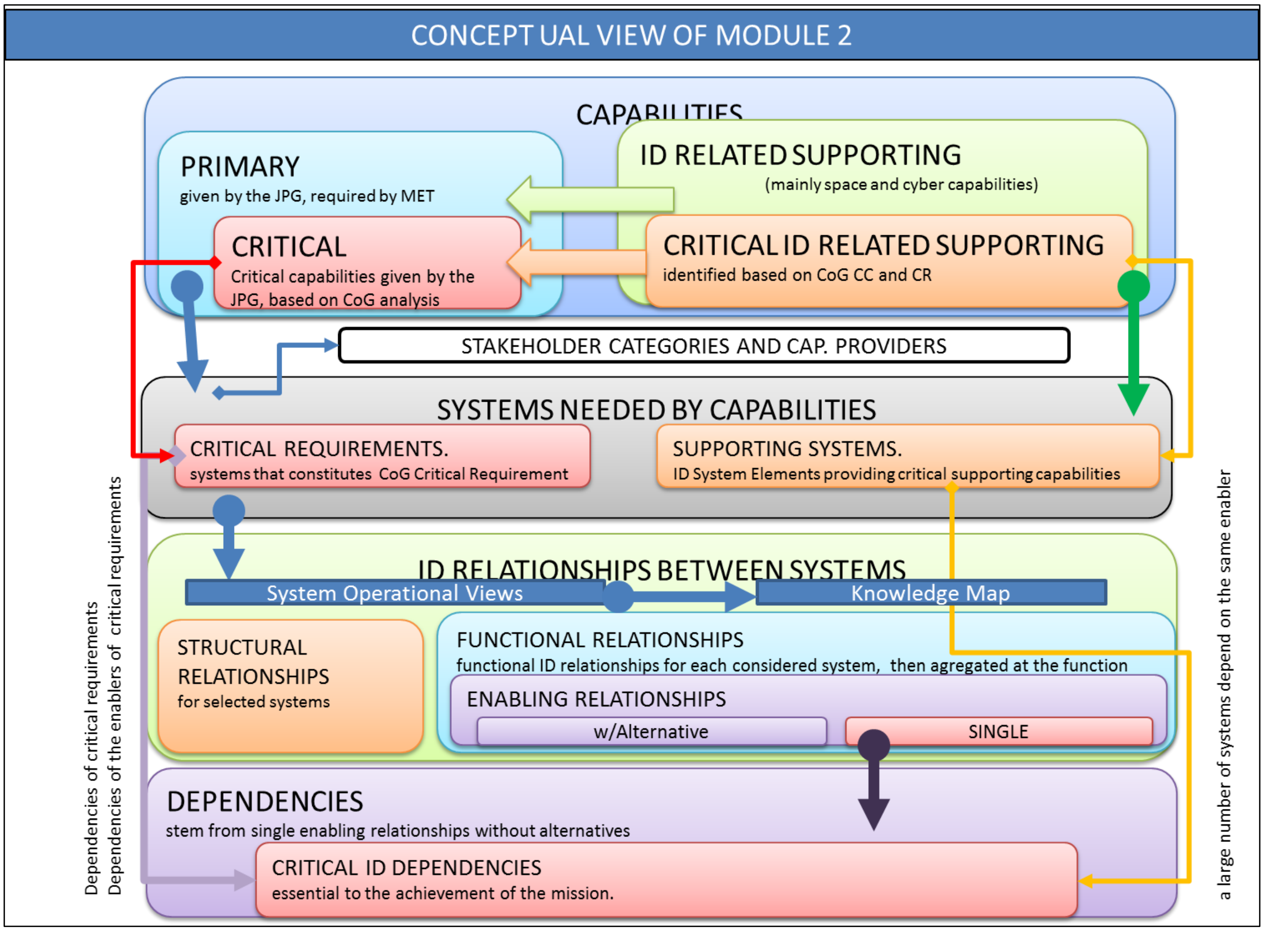
CONCEPT UAL VIEW OF MODULE 2
CAPABILITIES
PRIMARY
given by the JPG, required by MET
CRITICAL
Critical capabilities given by the JPG, based on CoG analysis
ID RELATED SUPPORTING
(mainly space and cyber capabilities)
CRITICAL ID RELATED SUPPORTING
identified based on CoG CC and CR
STAKEHOLDER CATEGORIES AND CAP. PROVIDERS
SYSTEMS NEEDED BY CAPABILITIES
CRITICAL REQUIREMENTS.
systems that constitutes CoG Critical Requirement
SUPPORTING SYSTEMS.
ID System Elements providing critical supporting capabilities
ID RELATIONSHIPS BETWEEN SYSTEMS
System Operational Views
Knowledge Map
STRUCTURAL RELATIONSHIPS
for selected systems
FUNCTIONAL RELATIONSHIPS
functional ID relationships for each considered system, then agregated at the function
ENABLING RELATIONSHIPS
w/Alternative
SINGLE
DEPENDENCIES
stem from single enabling relationships without alternatives
CRITICAL ID DEPENDENCIES
essential to the achievement of the mission.
Dependencies of critical requirements
Dependencies of the enablers of critical requirements
a large number of systems depend on the same enabler

Figure 5: Conceptual View of Module 2

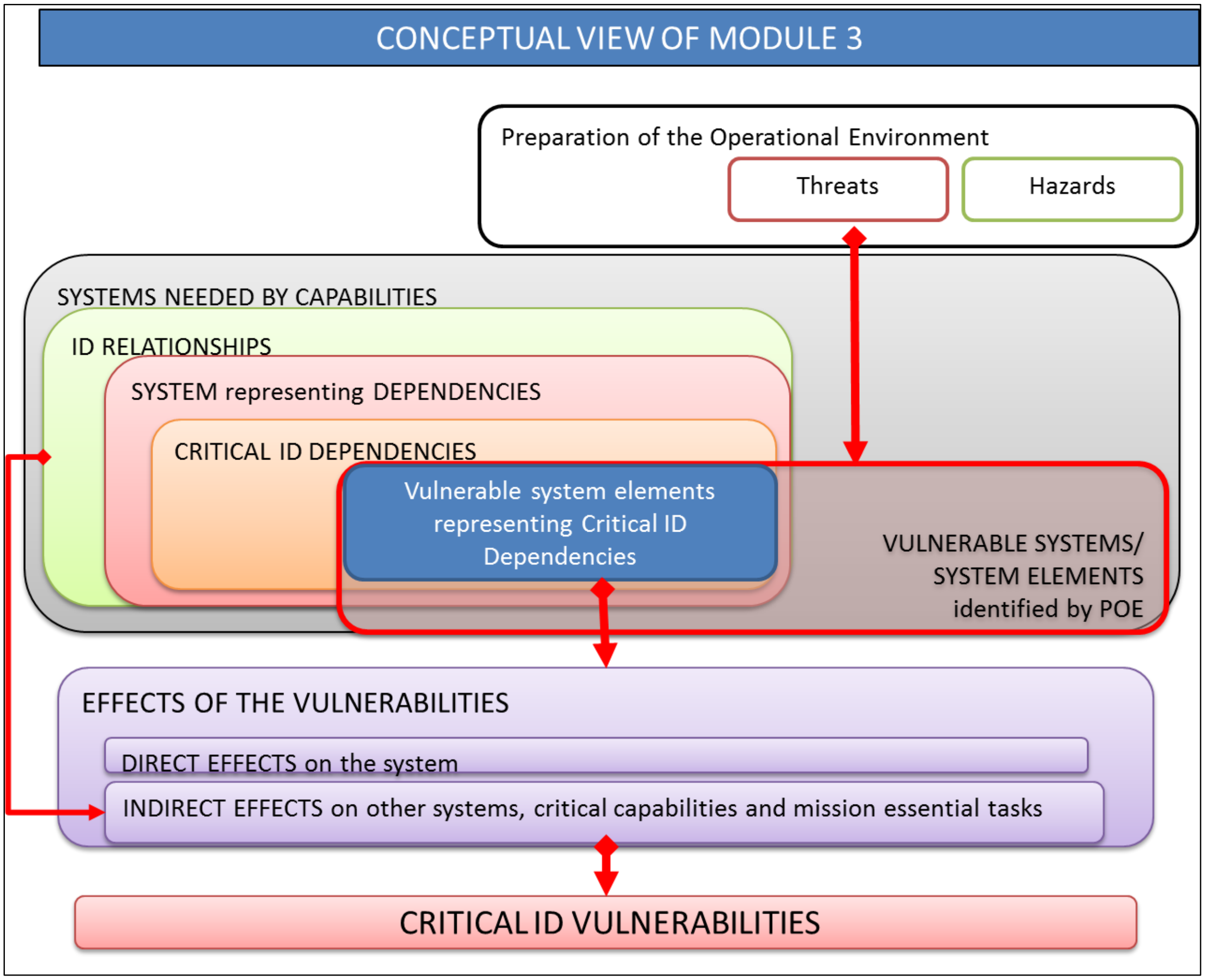
CONCEPTUAL VIEW OF MODULE 3
Preparation of the Operational Environment
Threats
Hazards
SYSTEMS NEEDED BY CAPABILITIES
ID RELATIONSHIPS
SYSTEM representing DEPENDENCIES
CRITICAL ID DEPENDENCIES
Vulnerable system elements representing Critical ID Dependencies
VULNERABLE SYSTEMS/ SYSTEM ELEMENTS identified by POE
EFFECTS OF THE VULNERABILITIES
DIRECT EFFECTS on the system
INDIRECT EFFECTS on other systems, critical capabilities and mission essential tasks
CRITICAL ID VULNERABILITIES

Figure 6: Module 3 Concept Card

For additional information regarding this methodology, please refer to MNE 7 Outcome 4: Methodology to Understand Inter-Domain Dependencies and Vulnerabilities, Guide version 1.0, 31 January 2013.

***

4- Potential DOTMLPFI Implications

Developing inter-domain understanding and incorporating this understanding in existing operational planning processes can have a number of implications. A first set of preliminary considerations, broken down here along the DOTMLPFI categories are provided below. These considerations are proposed by the MNE 7 Outcome 4 concept development team, drawing from the results of the work done during the MNE 7 campaign as "food for thought". Many of them relate to the potential implications of implementing the methodology described in the MNE 7 Outcome 4 guide. Further investigation of these issues would need to be undertaken before concrete recommendations for change could be made.

4.1 Doctrine

(a) The general notion of "inter-domain", or "cross-domain" considerations, as discussed in part 1 of this document ("The Military Problem"), should be considered for inclusion in various doctrinal publications, in order to enrich the description of the nature of the conditions under which military operations are taking place today.

(b) Provided that further evaluation of the concept and methodology developed in MNE 7 Outcome 4 confirms their value and applicability, specific inter-domain considerations could be incorporated into doctrinal publications.

- Key points of the methodology developed in MNE 7 Outcome 4 Methodology to Understand Inter-Domain Dependencies and Vulnerabilities, as well as organizational recommendations (see below) could be included into joint operations planning-related publications (doctrine and procedures).
- J6 publications could be adapted to take into account inter-domain considerations and stress the importance of including information systems and communications systems specialists in a process such as the one described in MNE 7 Outcome 4 guide.
- Given that the methodology is also intended to be applicable to Green and Red actors, key aspects from it, as well as its expected inputs and outputs, could also be tailored to better reflect the inter-domain perspective in joint intelligence and knowledge development–related publications particularly with regard to the preparation of the operational environment.
- Taken a step further, the analysis of a coalition's inter-domain vulnerabilities would require an evolution of the perimeter of KD given that the methodology proposed in the guide, has many components of KD, but, contrary to current KD, is focused on "Blue".

4.2 Organization

Using a methodology such as the one explained in the MNE 7 Outcome 4 Guide to identify a coalition's potential vulnerabilities in a given operational context could involve some adjustments in the conduct of staff work, since the methodology proposed is at the intersection of several functions. In the MNE 7 experimental context, the proposed solution was to set up an "inter-domain working group" within an operational staff, to work together with a joint planning group in order to identify inter-domain issues. Such a group would:

- Analyze of the coalition's inter-domain dependencies, in close support of the joint planning group, in order to identify the coalition potential critical ID vulnerabilities;
- Support intelligence and KD analysis of the adversary's and Green actors' inter-domain dependencies and vulnerabilities[24].

This type of inter-domain working group could be composed of:

- J5 or J35 planners:
  - To organize the interactions with the joint planning group;
  - To provide expertise on Blue systems.

- J6 planners:
  - To provide most of the expertise regarding the Blue information and communications systems;
  - To provide expertise regarding these systems' operating conditions as well as their knowledge of non-military cyber functions in the area of operations.

- J2/KD planners and experts, mainly required for the application of the methodology from the Blue perspective, to provide:
  - Expertise related to intelligence-related systems as well as the non-military domain functions in the area of interests;
  - Expertise on threats;
  - Systems analysis expertise to develop knowledge maps and analyze effects.

This type of working group would be complemented by other expertise within the staff based on the results of problem framing and the prioritized military functions to be worked on.

[24] This is not explicitly addressed in the methodology, though it has always been an assumption in MNE 7 Outcome 4 that this methodology could easily be adapted in order to analyze an adversary's inter-domain dependencies and potential vulnerabilities.

Moreover, reach-back mechanisms would need to be established:

- To space and cyber subject matter experts (SMEs) on the topics of:
    - Force contributing nations' capability providers
    - Non-military domain functions in the area of interest
- To force component staffs regarding Blue capabilities.

More broadly, given the increasing importance of cyber and space assets and the dependencies on them, there is great benefit to bringing space and cyber expertise more directly into the planning process[25]. Planners benefit from interactions with space and cyber experts who enable them to quickly spot potential risks associated with certain dependencies[26]. However, it is important to note that the availability of space and cyber remains a challenge from an organizational standpoint.

4.3 Training

The application of a methodology such as the one developed in MNE 7 Outcome 4 would require some training – both regarding its intellectual underpinnings as described in the conceptual framework and regarding the steps of each methodological module – in order to be implemented in a timely fashion during the operational planning process.

4.4 Material

The application of the MNE 7 Outcome 4 methodology to understand and map the inter-domain relationships among systems or assets could be enhanced by the development of specific data base applications capturing the key characteristics of these systems and assets from an inter-domain stand point.

For each system or asset, such database applications should be able to generate a corresponding diagram displaying the enabling inter-domain relationships. This diagram is called a "system operational view".

Systems databases should be populated in advance during peacetime by each interested nation based on existing information, such as data that is generated in a given system's technical documentation in the course of its development and operational life. Indeed, although the nature and level of inter-domain dependencies is generally context-dependent,

[25] During experimentation, both planners and experts highlighted the fact that they believed that this brought added value.

[26] Conversely, during the MNE 7 Outcome 4 Discovery Events and Limited Objective Experiment (LOE), space and cyber experts expressed satisfaction with and interest in being more directly associated with the planning process.

nonetheless, a number of standing inter-domain relationships between systems and elements remain unchanged regardless of the context.

Once the databases and associated systems operational views would have been established, they could be shared during the coalition planning process, according to the identified information exchange requirements[27]. By contributing to pre-identifying the standing systems or elements and their relationships, the databases and systems operational views would support the mapping of the operation specific ID relationships and subsequent analysis of the ID dependencies during the planning process (module 2 of the MNE 7 Outcome 4 methodology). They would provide analysts and planners with a solid basis from which to work when undertaking their representation of the ID System for a specific operation.

4.5 Leadership and Education

The process of bringing inter-domain issues into military decision-making processes above all requires raising awareness regarding the potential importance of inter-domain issues in particular the level of reliance on space and cyber. This can for example be done by incorporating an inter-domain component to Joint Staff College exercises.

4.6 Personnel

It is assumed that the implementation of a methodology to understand inter-domain vulnerabilities requires bringing together intelligence and/or knowledge development expertise, planning expertise (J5, J3 and J6) as well as cyber and space expertise, through local liaison or reach back (See “Organization”, above).

4.7 Facilities

N/A.

4.8 Interoperability

Developing databases that could easily be shared and used for the purposes of mapping and analyzing a coalition’s inter-domain dependencies and vulnerabilities – as described in the “Material” section – would necessitate an effort in terms of interoperability. Furthermore, given the reluctance to share information regarding the vulnerability of systems, even among allies and partners, developing an understanding of friendly inter-domain

[27] It is recognized that this type of database would likely be classified. Sharing the information in this type of database would therefore require specific information-sharing agreements.

vulnerabilities in a coalition environment will require a level of information-sharing and trust.

5- Risks

There are a number of risks worth noting, as related to:

- The context of MNE 7,
- Building inter-domain understanding,
- Some of the more concrete implications.

Regarding the MNE 7 context, it is important to note that while the results of experimentation pointed to the added value of the methodology, not all of its steps and sub-steps were thoroughly examined. Therefore further evaluation of the methodology would be needed before incorporating it into staff procedures.

While there appears to be an emerging consensus regarding the need to better take into account cyber and space and to enable interactions between planners and technical experts in these subjects, the best way to do so remains to be determined. The Outcome 4 methodology provides one way of potentially proceeding.

As stated in the sub-section related to interoperability, some risks also relate to the willingness to share information regarding vulnerabilities. Furthermore, in a coalition context, incorrect information related to the vulnerability of a given system could lead to incorrect analysis of the chains of effects and therefore of the critical inter-domain vulnerabilities of an operation.

Intentionally Blank

Part 3 – Illustrative Examples

1- Ailamos Illustrative Example

Please note: the sole purpose of this fictional example is to highlight the importance of inter-domain (ID) issues and the type of insights that could emerge by taking them into account within a planning process in a structured manner using a methodology such as the one developed in MNE 7 Outcome 4. While the example mentions real systems in order to make the illustration more tangible, it is NOT intended to portray any real enabling relationships or dependencies between these systems. All data used to describe systems was taken from open, unclassified sources and does not strive for accuracy in describing these specific capabilities.

1.1 Context

During a period of drought, leading to widespread food shortages, a religious fundamentalist terrorist group named Al Shaebi in the country of Ailamos has expanded its power over the local population. Al Shaebi derives significant income from trafficking of weapons, drugs and humans. In order to expand its reach and visibility on the world stage, Al Shaebi reaches out to other fundamentalist groups within the region. It develops connections with these groups by offering training sites and other support. Al Shaebi develops a cyber warfare capability by exploiting its connections with other regional terrorists to tap into pools of cyber expertise.

Believing that the humanitarian relief effort is a nuisance to their activities and control over the population, Al Shaebi begins a concerted effort to discourage relief organizations from operating in the territories it controls. Thus, international relief efforts in Ailamos are almost halted as humanitarian aid workers are increasingly harassed and attacked as targets of the Al Shaebi terrorist group. The Al Shaebi strategy is to attack and take supplies from the NGOs in the area and then reward their followers with the spoils, while starving the non-supporting population.

In response to the escalating famine and Al Shaebi attacks, the United Nations Security Council passes a resolution condemning the attacks and asking states and regional organizations to provide security to enable the distribution of aid. The UN peacekeeping forces in the region are increasingly ineffective, lacking the force structure or capacity to maintain security for relief efforts with the growing violence in the region. Following a UN request, the North Atlantic Council (NAC) agrees to send military forces to provide security for humanitarian relief efforts in the region. The forces deployed to the area are limited to a mobile infantry brigade and supporting rotary and fixed wing aviation elements, not counting a small naval support component.

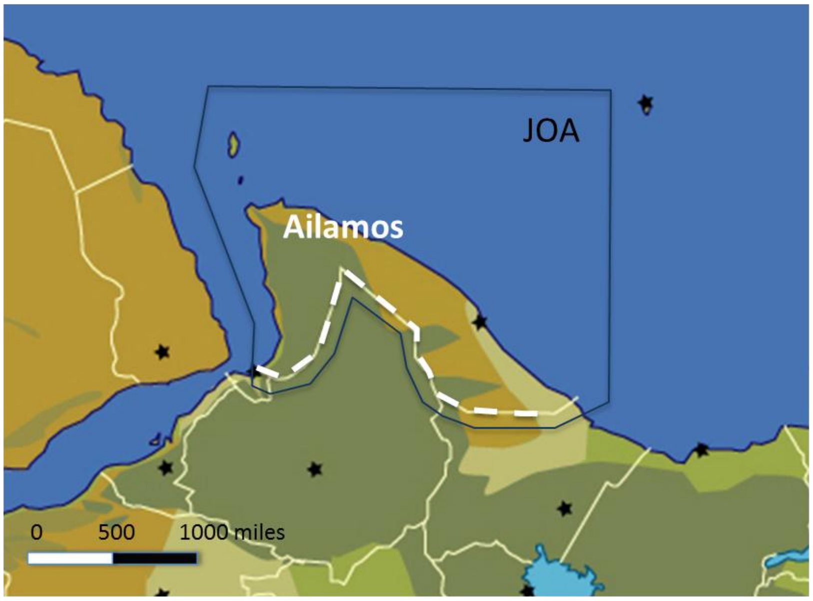

Figure 7: Map of Ailamos and the NATO Forces Joint Operation Area

1.2 Potential Inter-Domain Aspects of the Operation

Even in an operation involving an opponent with fairly limited capabilities, an inter-domain dimension might be at play. An adversary such as Al Shaebi could count on cyber experts and hackers through international contacts and possess tactical jammers. Used together, these could create significant difficulties for a coalition, due in particular to the size of the area of operations and the fairly limited number of troops available.

Cyber means could be used to deceive coalition actors and gain a tactical advantage. It is fairly clear that in this context, C2 (to include civil-military linkages) is particularly important; an adversary could therefore seek to target the coalition's C2 through exploitation and spoofing, taking advantage of the potential weak spots at the interface of military and civilian networks in the joint operation area.

1.3 Value of the methodology

In this example, the methodology proposed in MNE 7 Outcome 4 would add value in several ways.

First, as part of the problem framing, the methodology provides a way for the commander and his staff to begin taking into account inter-domain aspects of the operation.

In this case, as part of the normal planning process, the coalition planning staff and the commander would have already recognized that significant challenges stem from the size of the area of operations and the fairly limited number of troops at their disposal, as well as the importance of securing the main ports and airfields. They would also consider that Al Shaebi's intent could likely be to undermine the cohesion among stakeholders and the legitimacy of the military intervention in addition to increasing their own power in the area.

The initial preparation of the operational environment (POE) briefing would show that Al Shaebi have been seeking to hire cyber experts through their international contacts, but little more would be known on this topic. The POE would also show that they have purchased a number of different types of tactical jammers, including GPS, standard radio and SATCOM jammers from the black market and that they are skilled in the use of communications interception and jamming against local humanitarian aid providers.

Given the environment, the theater constraints and the adversary capabilities, by applying **module 1 of the methodology ("framing the inter-domain dimension of the engagement"),** the commander would orient his staff to investigate the following inter-domain issues:

1) How can the adversary's tactical jamming assets and cyber expertise directly affect the coalition's C2 and Fires functions?
2) How can the adversary use these capabilities, according to an indirect approach, to exploit civilian systems in order to affect coalition functions?

The main functions to be considered are Command and Control (with a particular focus on civil-military coordination with national civilian actors, international organizations, NGOs and local authorities), Fires, Movement and Maneuver, and Sustainment.

***

In addition to these inter-domain issues, the commander and his staff could assess the coalition's strategic Center of Gravity (CoG) as the cohesion and coordination of stakeholders and the operational CoG as the brigade ability to act in a distributed fashion over a large area with speed and mobility and to coordinate with civilian partners. The Mission Essential Tasks (MET) could be:

1) Escort and protect humanitarian aid
2) Protect the critical lines of communication
3) Secure areas of special interest
4) Create situational awareness (joint operating picture)
5) Coordinate MET 1-4 with civilian organizations.

In addition to the traditional CoG analysis, according to **module 2 of the methodology ("ID relationships mapping and ID dependencies analysis")**, an effort would be made to identify the critical ID-related supporting capabilities such as "deploy distributed C2 network", "ability to share information with civilian actors" and "ability to protect SPOD, air and maritime approaches" and to use these to refine the CoG CC and CR.

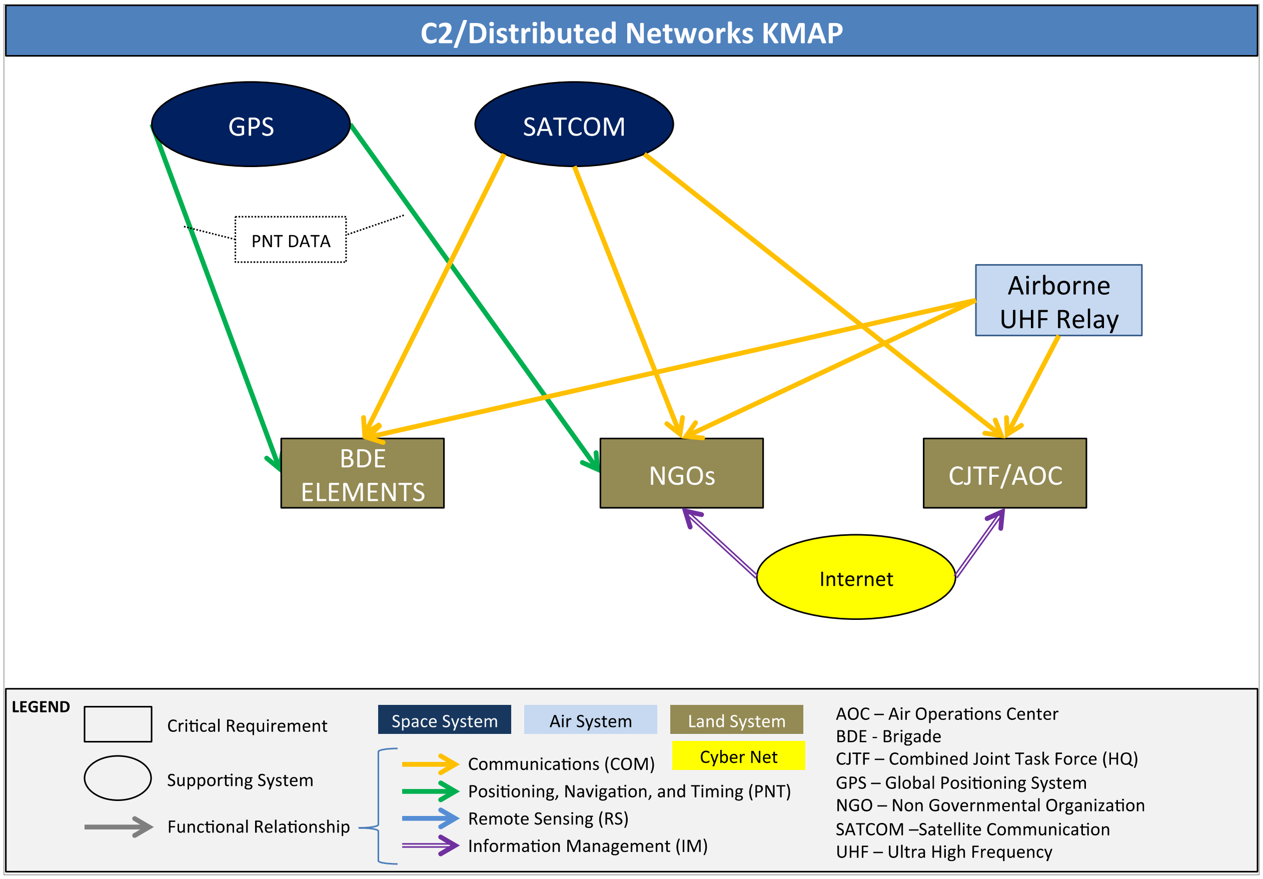
C2/Distributed Networks KMAP
GPS
SATCOM
PNT DATA
Airborne UHF Relay
BDE ELEMENTS
NGOs
CJTF/AOC
Internet
LEGEND
Critical Requirement
Supporting System
Functional Relationship
Space System
Air System
Land System
Cyber Net
Communications (COM)
Positioning, Navigation, and Timing (PNT)
Remote Sensing (RS)
Information Management (IM)
AOC – Air Operations Center
BDE - Brigade
CJTF – Combined Joint Task Force (HQ)
GPS – Global Positioning System
NGO – Non Governmental Organization
SATCOM –Satellite Communication
UHF – Ultra High Frequency

Figure 8: Partial Knowledge Map (Kmap) of the Force C2/Distributed Networks.

Moreover, the methodology in module 2 would lead to a mapping of the relationships, through the use of Knowledge Maps (Kmap), as depicted above, and an analysis of the dependencies related to the C2 (focusing on CIMIC interface related supporting BLOS communications capabilities), Fires (focusing on JTAC supporting capabilities, such as radio networks), Movement and Maneuver (focusing on transport helicopters supporting capabilities, PNT and communications) and Sustainment (focusing on port communications) functions. This could highlight the critical dependency of the CIMIC interface on the Internet or the critical dependency on the Iridium satellite constellation for its BLOS communications.

***

The analysis of the chains of effects stemming from potential threats or hazards as proposed in **module 3 of the methodology ("critical ID vulnerabilities identification")** could then help to understand the impact of a jamming of GPS and radio systems, of cyber activities directed at the CIMIC interface capabilities, and of the spoofing of specific SATCOM on the ability to perform essential tasks.

The correlation of the effects would lead to a better understanding of the adversary's potential courses of action. For example, the adversary could seek to exploit the linkages between the military and other stakeholders: Al Shaebi operators could track a variety of NGOs' activities through their Iridium connection or SAT phones. They could use an NGO as an entry point as a way to "see into" operations and then use a portal (such as a medical portal or virtual coordination center) to feed incorrect data (for example, regarding need to protect X convoy going to Y location) in order to set up an attack. Once Al Shaebi had gotten forces to go to the location it wants, it could stage an attack, using tactical jammers to block and blind Blue C2 and Fires. This type of cyber-enabled ambush would be a classic case of using operational deception to gain tactical superiority. If this attack succeeded, it would have a twofold effect: 1) casualties could have negative impact on public opinion and affect cohesiveness among stakeholders 2) as a result, the commander would be reluctant to send out small units and would mass forces; as a result, the forces would be able to cover over less territory, thereby giving the adversary greater freedom of maneuver.

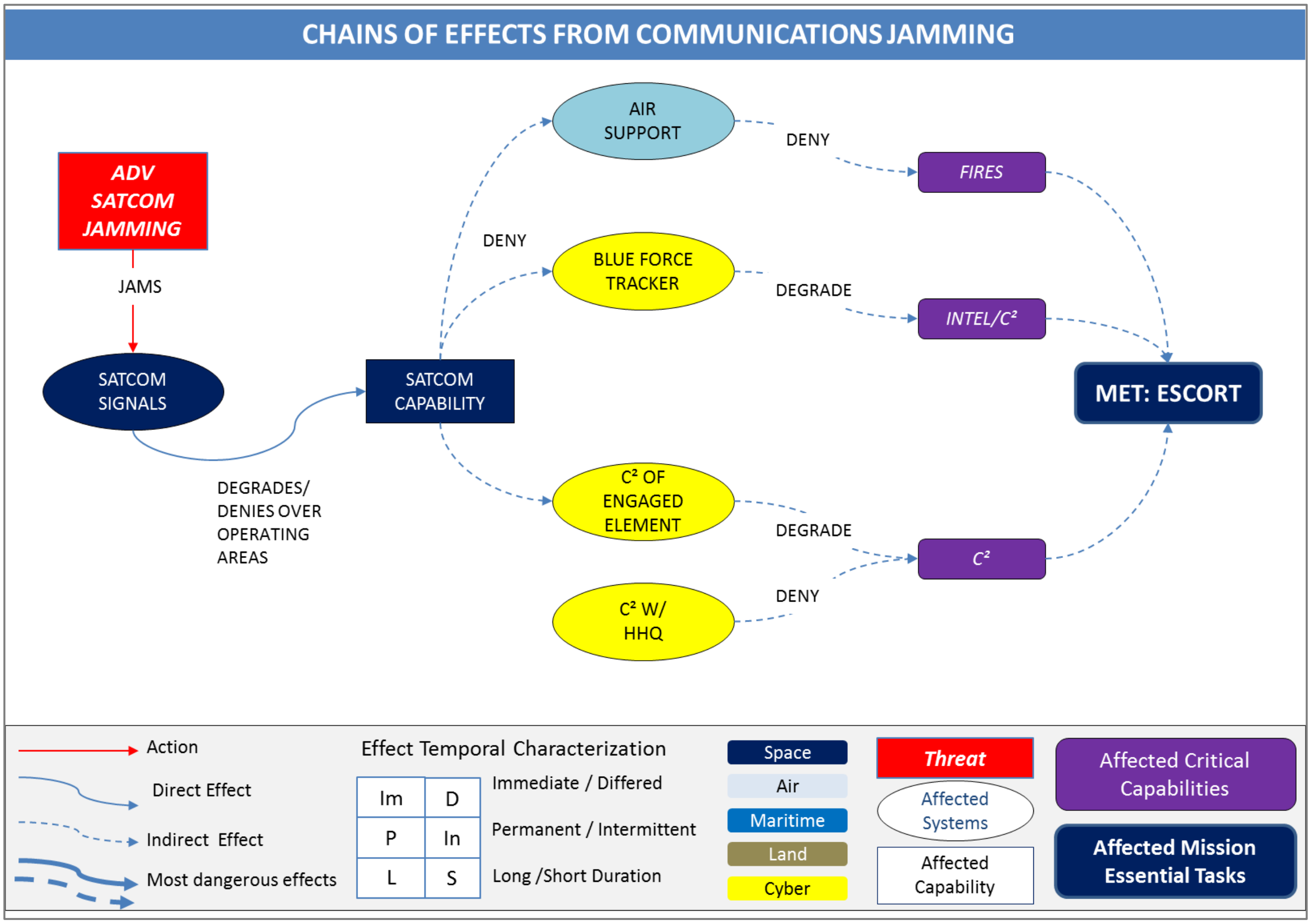

Figure 9: Sample Diagram of Influence Depicting the Chains of Effects that could Result from Communications Jamming

The identification of such critical vulnerabilities would enable the commander to seek out mitigation options. These could involve looking at alternative communications means for the civilian actors or additional procedures for civil-military communications. The analysis of the Fires function could highlight the susceptibility to jamming and also lead the commander to seek out mitigation options.

2- Aybil Illustrative Example

Please note: the purpose of this fictional example is to highlight the importance of inter-domain (ID) issues and to illustrate how their systematic consideration during an operational planning process – which is the aim of the MNE 7 Outcome 4 Methodology – would help shape a more robust plan. While the example mentions real systems in order to make the illustration more tangible, it is NOT intended to portray any real dependencies or vulnerabilities between these systems. All technical data used to describe systems was taken from open, unclassified sources and is not necessarily accurate.

2.1 Context

A rebellion in the Mediterranean country of Aybil has the aim of overthrowing the long ruling dictator, Major Kaffey. The citizens of Aybil support the rebellion and some of the armed forces defect to support the insurrection. The rebellion uses social media through satellite and other Internet connectivity to provide intelligence and command and control for its forces. To avoid Aybil's strict cyber censorship, the rebel forces have utilized an Internet provider in neighboring Tpyge to maintain communications with the outside world. Major Kaffey, on the other hand, possesses ballistic missiles, cyber capabilities and satellite jamming assets in addition to extensive traditional military forces. Major Kaffey has shown his willingness to use military action, including air strikes and heavy artillery, against his own people.

The United Nations Security Council passes a resolution calling for an immediate ceasefire to protect Aybil's civilian population and for the establishment of a no-fly zone over Aybil. The North Atlantic Council decides that NATO will conduct military operations to enforce the no-fly zone and protect Aybil's population.

NATO members are ready to provide not only air forces, but also ships and ground forces to maintain tactical flexibility. The Combined Joint Task Force (CJTF) headquarters is set up on the USS Mount Whitney. This ship also hosts the maritime component commander and his staff. The U.S. provides additional combat ships, to include three Aegis, ballistic missile defense (BMD) capable, cruisers. The majority of U.S. and European air assets supporting the CJTF are land-based and distributed throughout the Mediterranean bordering countries. The Combined Air Operations Center (CAOC) is separated geographically from the CJTF commander and is located in Ramstein, Germany. The US has offered a TPY-2 ground-based BMD tracking radar to deploy in the area to enhance the missile defense capabilities of the coalition.

Before the coalition can establish the no-fly zone over Aybil, two conditions must be met. First, the threat of ballistic missiles that can reach some of Aybil's neighboring countries and NATO support bases must be diminished by putting in place a layered active missile defense to protect partners and supporters. If this condition is not met the coalition might not hold together long enough to conduct operations. Second, the enemy air defense capabilities must be suppressed or destroyed so that NATO can achieve the required air superiority. Precise intelligence, surveillance, and reconnaissance (ISR) data and long range, stand-off fires are required to nullify Aybil's air defenses before air assets can patrol Aybil's airspace.

***

As the traditional crisis action planning process progresses, the planning staff determines the Blue center of gravity (CoG) to be the layered active BMD to protect Blue and Green countries within the threat ring of Aybil's ballistic missiles. Without this capability, Aybil can use their ballistic missiles to undermine the cohesiveness of the coalition and the coalition supporters' will to continue to support the rebel forces. The intelligence and knowledge development products also underline that Aybil has great familiarity with some of its immediate neighbors' infrastructure, including in the cyber domain, and could take advantage of this to influence their support of the ongoing rebellion and NATO intervention.

Note: What follows centers on the BMD issue and the Green infrastructure concerns in order to provide a focus for this illustrative example, understanding that there would be other mission essential tasks and critical capabilities that would be taken into account as part of the planning process.

2.2 Ballistic Missile Defense

In the course of the normal operational planning process, the CJTF staff determines that Major Kaffey has two main courses of action concerning his ballistic missile capability:

1) To launch the missiles to inflict damage on Blue and Green countries so that the latter will pressure the coalition to cease actions to avoid more damage;
2) To keep the ballistic missiles as a force in being so that the threat of their usage can be used to weaken or disband the coalition.

There are three Blue critical capabilities to support BMD:

1) The ability to detect and track a ballistic missile launch;
2) The ability to command and control all of the BMD systems;
3) The ability to engage and destroy incoming ballistic missiles.

After evaluating these three capabilities, the application of an inter-domain focused methodology such as the one developed in MNE 7 Outcome 4 would highlight the fact that assured satellite communications (SATCOM) to pass cueing data to the interceptors is a critical inter-domain related supporting capability for which there is no alternative in relation to the BMD mission.

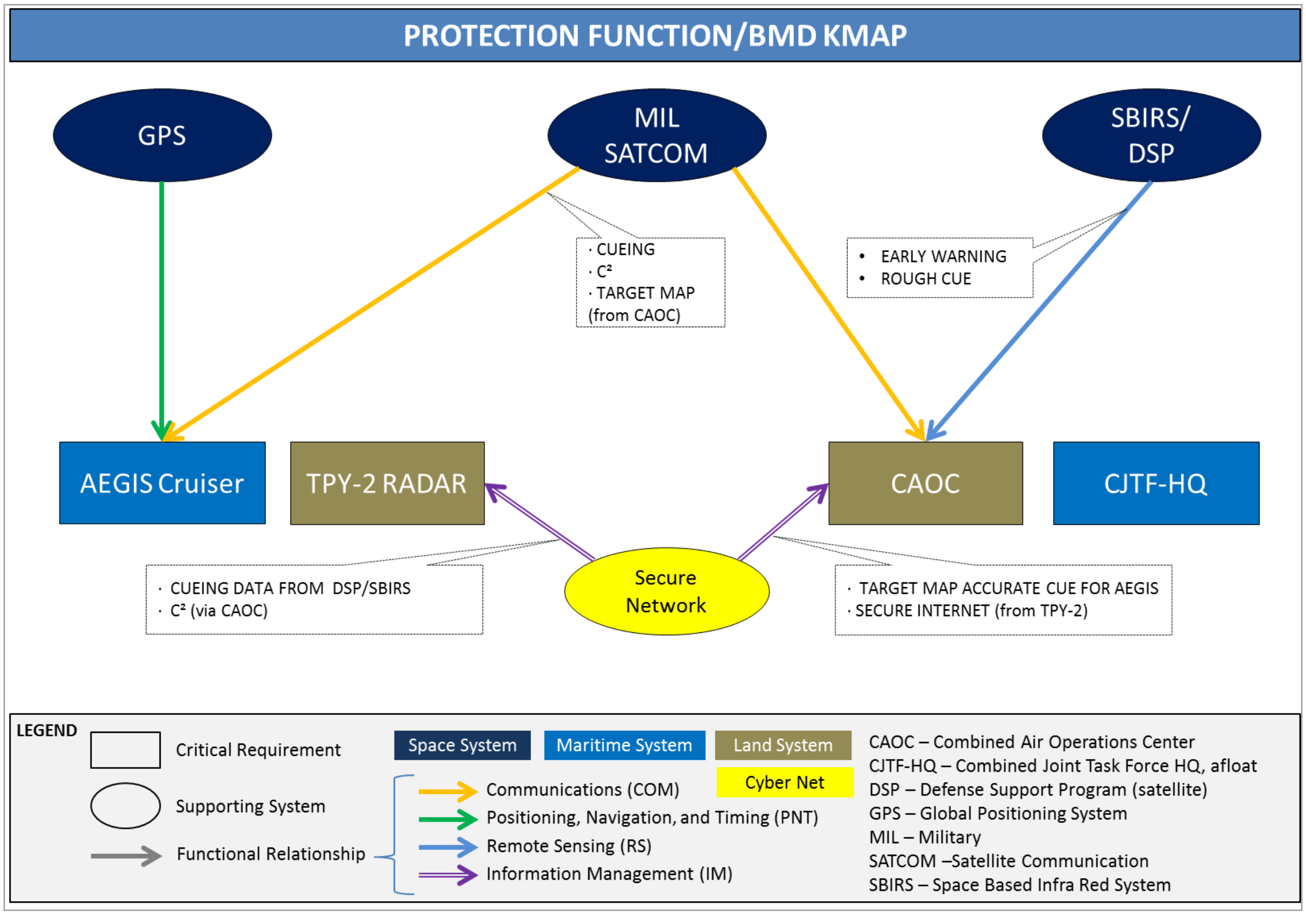
PROTECTION FUNCTION/BMD KMAP
GPS
MIL SATCOM
SBIRS/ DSP
· CUEING
· C²
· TARGET MAP (from CAOC)
• EARLY WARNING
• ROUGH CUE
AEGIS Cruiser
TPY-2 RADAR
CAOC
CJTF-HQ
Secure Network
· CUEING DATA FROM DSP/SBIRS
· C² (via CAOC)
· TARGET MAP ACCURATE CUE FOR AEGIS
· SECURE INTERNET (from TPY-2)
LEGEND
Critical Requirement
Supporting System
Functional Relationship
Space System
Maritime System
Land System
Cyber Net
Communications (COM)
Positioning, Navigation, and Timing (PNT)
Remote Sensing (RS)
Information Management (IM)
CAOC – Combined Air Operations Center
CJTF-HQ – Combined Joint Task Force HQ, afloat
DSP – Defense Support Program (satellite)
GPS – Global Positioning System
MIL – Military
SATCOM –Satellite Communication
SBIRS – Space Based Infra Red System

Figure 10: Notional Kmap Depicting the Inter-Domain Relationships for BMD

Therefore, the SATCOM link would be identified as a critical inter-domain dependency. After this, in light of the threat of Aybil's satellite jamming capability, this inter-domain dependency would be categorized as a critical inter-domain vulnerability for the operation. This in turn would feed the course of action development phase, during which the CJTF commander and his staff would have an opportunity to design operations to mitigate this vulnerability. In this situation, they would be aware, early in the planning process, of the need to ensure the proper prioritization of jam resistant SATCOM for BMD cueing data, as well as of ISR and strike missions targeting satellite jammers.

2.3 Green Nation Infrastructure

Another inter-domain issue that the CJTF staff would explore could be the impact of Aybil's computer network operations (CNO) capability on the neighboring Green nations' infrastructure. Based on intelligence and knowledge development products, the staff would recognize that Aybil had helped the other nations in the region develop their electrical, water, transportation and cyber network infrastructure. This would give Aybil unprecedented access to and intelligence about these systems. Aybil's CNO capability could be used to attack neighboring Green countries to bully them into not supporting the coalition. It could also be used to attack the neighboring countries' cyber connectivity providers that the Aybil rebels use to communicate with the coalition.

By following the methodology, the planning staff would identify that a critical inter-domain dependency for the operation is the cyber connectivity that the rebels have through a Tpyge Internet provider as their main communication link to coordinate with the coalition. Analyzing this inter-domain dependency relative to the Aybil threat of computer network operations against Tpyge Internet connections would show this inter-domain dependency to be a critical inter-domain vulnerability of the operation.

During the course of action development process, the CJTF commander and staff would have an opportunity to address this vulnerability. The staff could then for example alert the Tpyge Internet provider to increase their security (both virtual and physical) and the CJTF could request the deployment of a NATO Cyber Rapid Reaction team to the provider to augment their organic cyber protection resources.

2.4 Conclusion

As this example shows, a formal methodology like the one developed in MNE 7 Outcome 4 would allow the staff to conduct a systematic, mission-related analysis of inter-domain dependencies and evaluate them in light of specific threats, hazards, and operating conditions to reveal critical inter-domain vulnerabilities specific to a given operation. In turn, this would allow the operational commander and his or her staff to take appropriate actions in the development of their course of action to mitigate these inter-domain vulnerabilities.

***

Intentionally Blank

Appendix A: Generic ID-related Capabilities

This appendix proposes a list of generic ID-related capabilities related to each of the domains.

Space Domain

Three of the four "pillars" of space (defined in MNE 7 Outcome 2 as PNT, Communications, ISR and Space Situational Awareness) are currently dedicated to supporting or countering activities in geographic and cyber domains and are therefore inter-domain:

- Satellite communication (SATCOM) capabilities, either civilian or military ones, the main source of Beyond Line of Sight (BLOS) communications;
- Positioning, Navigation and Timing (PNT);
- ISR, to be understood as the space-based remote sensing and associated processing capabilities and encompassing the traditional collection disciplines:
    - Imagery Intelligence (IMINT),
    - Signals Intelligence (SIGINT), including communications and electronic intelligence,
    - Measurement and Signature (MASINT) including missile warning capabilities and other remote sensing capabilities, including weather support.

(For further information, please refer to Outcome 2, Objective 2.1 publication entitled "Space: Dependencies, Vulnerabilities and Threats").

Maritime Domain

From a maritime domain perspective, ID-related capabilities include:

- Points of entry for space and air activities (provided by all maritime platforms embarking air assets or able to launch spacecraft);
- ISR collection and associated processing capabilities provided by ships, submarines, or other maritime domain elements;
- Counterair capabilities, including air and missile defense, provided by naval assets;
- Command and control nodes provided by ships;
- Information operations capabilities including PSYOP/MISO and EW performed by naval assets;
- Naval interdiction and special operations capabilities against land-based space points of entry, control segment facilities of space subsystems and cyber domain physical sites.

- Wired communications (undersea cable networks).

Air Domain

From an air domain perspective, ID-related capabilities include:

- Command and control, and communication nodes provided by air assets (including AWACS UAVs used as communication relays);
- ISR collection provided by air sensors and associated processing capabilities;
- Countersea capabilities including anti-surface, anti-submarine, mine laying warfare capabilities;
- Information operations capabilities that may be performed by air assets including
  - PSYOP/MISO;
  - EW;
- Air interdiction and special operations capabilities against land-based space points of entry, control segment facilities of space subsystems and cyber domain physical sites.

Cyber Domain

Most activities executed in the cyber domain have a strong ID dimensions: on one hand, every network has a physical layer relying on one or more physical domains, on the other hand, cyber activities increasingly affect, directly and indirectly, most activities performed in the other domains.

The following Cyber capabilities are drawn from US DoD Net-Centric Joint Capabilities Area:

- Information transport: "*The ability to transport information and services via assured end-to-end connectivity across the [cyber] environment*", which encompasses wired and wireless transmission of data, switching and routing. Information transport includes Beyond Line of Sight (provided by SATCOMs), Line of Sight and Wired communications capability;
- Enterprise services: *The ability to provide to all authorized users awareness of and access to all [relevant] information and […] information services*. Such "services" include PNT;
- Net management: "*The ability to configure and re-configure networks, services and the underlying physical assets that provide end-user services, as well as connectivity to enterprise application services*";
- Information assurance: "*The ability to provide the measures that protect, defend and restore information and information systems*"[28].

[28] US Joint Staff, *Joint Capability Areas*, JCA 2010 Refinement approved 8 April 2011, pages 38-42.

Offensive/defensive cyber ID capabilities include:

- PSYOP/MISO or influence activities;
- Electronic warfare;
- Computer network operations (CNO), encompassing Computer Network Attack, Defense and Support.

Land Domain

Most land domain capabilities have an inter-domain dimension depending on the context. It includes:

- The capabilities which have an direct effect on other domain activities: the command and control of joint operations, land-based information collection (provided by very diverse assets: air early warning radars, space surveillance assets), defensive counter-air capabilities (surface-to-air capabilities), land-based air naval operations, etc.;
- The supporting capabilities that have an indirect effect on the activities in the other domains: logistics, transportation networks, etc.

Moreover, the following inter-domain assets, connecting land domain to other domains should be considered:

- seaports,
- airports,
- space launching and ground segment facilities, as well as spacecraft (i.e. electronic warfare, laser binding, or electromagnetic pulse),
- cyber facilities (data centers, wired communication, radio relay communications, etc.).

Points of Contact:

Lt Col Philippe COQUET
MNE 7 FRA National Director
Centre Interarmées de Concepts, de Doctrines et d'Expérimentations
E-mail: philippe.coquet@intradef.gouv.fr
Phone: + 33 1 44 42 82 71

Mr. Philippe GROS
MNE 7 Outcome 4 Concept Developer
Fondation pour la recherche stratégique
E-mail: p.gros@frstrategie.org
Mobile Phone: + 33 6 16 61 04 02
Work Phone: + 33 1 43 13 77 87

Mrs. Anne KOVACS
MNE 7 Outcome 4 Project Lead
U.S.-CREST
E-mail: anne.kovacs@uscrest.org
Phone: + 1 703 243 6908

Mr. Dominique ORSINI
MNE 7 FRA Lead Analyst
U.S.-CREST
E-mail: dorsini@uscrest.org
Phone: + 1 703 243 6908