Paper Submission for the 23rd International Command and Control Research and Technology Symposium
(Pensacola, FL / 2018)

Paper No. 80

CONCEPT PAPER

The Mission Value Pyramid: A Framework for Basic Research Supporting C2, with Examples

Marius S. Vassiliou
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria VA 22311
USA
mariusvassiliou@gmail.com

David S. Alberts
Strategy, Forces, and Resources Division
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria VA 22311
USA
davidsalberts@gmail.com

Keywords: C2; Command and Control; Basic Research; Mission Success; Communications

Abstract

We present a conceptual framework, the "Mission Value Pyramid," for success in command, control and communications of complex missions, and use it to identify some example areas for basic research supporting the fundamentals of mission success. In the framework, mission success depends on adopting appropriate approaches to Command and Control, which depends in turn on effective management and use of complex, composite, multi-genre sociotechnical networks. These depend on effective and agile component networks, buttressed by assured communications capability. At lower levels of the Mission Value Pyramid, concerned with assured communications, some of the areas we identify include information theory for general, multi-hop, wireless mobile networks; mathematical treatment of multiple heterogeneous networks and their interconnection protocols; sub-Turing languages for cyber security; and new mathematics with applicability to encryption. At higher levels of the Pyramid, important areas include achieving a fundamental understanding of the behavior of composite networks, including trust dynamics. The understanding of systemic risk, and phenomena such as the normalization of deviance, are also important. The topics presented here do not constitute an exhaustive set, and many more are possible and desirable. We do not touch on some important areas such as data analytics, for example. The topics are also not prioritized. The main goal of this paper is to present a conceptual framework and begin to identify some important basic research topics and how they fit together.

1. Introduction

The United States Department of Defense (DoD) defines Basic Research[1] as "systematic study directed toward greater knowledge or understanding of the fundamental aspects of phenomena and of observable facts without specific applications towards processes or products in mind.' However, unlike other commonly accepted definitions of Basic Research[2], the DoD definition explicitly specifies that the "scientific study" be "directed toward increasing fundamental knowledge and understanding in those fields of the physical, engineering, environmental, and life sciences related to long-term national security needs." The definition also characterizes basic research as providing "the basis for technological progress," and it suggests that basic research "may lead to […]new and improved military functional capabilities in areas such as communications, detection, tracking, surveillance, propulsion, mobility, guidance and control, navigation, energy conversion, materials and structures, and personnel support."

In this paper we follow the spirit of the above definition, and explore some areas of basic research, in a number of sciences, that have the potential to improve U.S. military mission success through better Command, Control, Communications, and related areas. We consider topics in applied mathematics, information theory, computer science, and emerging disciplines such as network theory that may involve social sciences and psychology as well. In preparing this paper, we have drawn on our own experience, conducted additional research, and consulted with several experts.[3]

---

[1] DOD (2016)

[2] E.g. OECD (2002)

[3] We acknowledge helpful discussions with Prof. Ali Jadbabaie of MIT; Profs. Jeffrey Reed, Harpreet Dhillon, Jerry Park, and Tom Hou of Virginia Tech; Prof. Jean-Pierre Benoit of the London Business School; Dr. Joe Mitola of the

The areas outlined here do not constitute an exhaustive set, and many others are possible and desirable. We present an overall framework for understanding how the various topic areas—both the examples we discuss here and future ones that may be suggested by others—fit together in their long term potential to create a better future edifice for military mission planning and execution.

2. Framework: The Mission Value Pyramid

2.1 The Right Information at the Right Time to the Right Actor

As shown by a broad variety of experiences and scientific studies[4], successful complex endeavors (such as many military missions) depend crucially on the selection of the appropriate Command-and-Control (C2) or enterprise approach, buttressed by assured communications capability.

One of the important ways enterprise approaches in complex missions go wrong is that they fail to get the right information to the right individuals at the right time[5]. This "right information" may not always be in the form of massive multimedia files, or even buried therein. Sometimes, it may be as simple as a "yes" or "no," or other compact form. As studies have also shown, the underlying reasons for these failures have as much to do with organizations that do not exhibit agile behaviors as they do with technical communications failures.

2.2 An Illustrative Example

As an illustrative example, consider the problems encountered during the failed US attempt (24-25 April 1980) to rescue the American hostages being held in the United States embassy in Tehran, Iran.[6]

During the mission, a C-130 transport airplane heading to the rendezvous landing site ("Desert One") encountered a large desert dust cloud (known in Iran as a *haboob*). The *haboob* was not a major problem for the airplane, but it was potentially a serious threat to the eight helicopters following far behind it. The airplane did not warn the helicopters because of a strict dictate of radio silence. There was a chance the aircrew could have used a secure satellite radio to issue the warning, but unfamiliarity with the equipment made them unable to work out the coding parameters.

The helicopters thus entered the *haboob*. Because of radio silence, they could not tell each other what they were doing or where they were going. One helicopter had to abort because of a suspected blade failure, and two others left the *haboob* and landed. One of the two that landed prematurely was that of the group's leader. The leader made a secure call to a U.S. command center in Egypt and was told to proceed to the rendezvous landing site, but none of the other helicopters could hear the conversation. The other pilot that had landed prematurely was no longer in visual contact.

Hume Center; Dr. Cynthia Dion-Schwarz of the RAND Corporation; Dr. Syed Shah of the Office of the Assistant Secretary of Defense for Research and Engineering (OASD(R&E)); and Mr. David Jakubek, formerly of OASD(R&E).

[4] Vassiliou et al. (2015); Alberts (2011); NATO (2013)

[5] Vassiliou et al. (2015); Vassiliou and Alberts (2013)

[6] Anno and Einspahr (1988); Bowden (2006)

Because of readings indicating malfunctions and the difficulty of flying again through the *haboob*, he made an independent decision to return to the aircraft carrier *Nimitz*. To make things worse, his was the helicopter carrying all the spare parts needed for possible repairs. None of the helicopters could talk directly to Desert One and thereby learn that the rendezvous landing site was clear. Later, the pilot who returned said he would have continued had he known that fact. The inability to communicate led to the loss of needed helicopters and crucial spare parts at Desert One. The mission was canceled on the ground after several other missteps, and during the retreat one of the helicopters collided with one of the transport planes, killing eight soldiers.

The failed mission also had a number of organizational and structural problems. It involved U.S. Army Delta Force, U.S. Army Rangers, U.S. Air Force pilots, and U.S. Navy helicopter pilots, among others, in a highly complex operation. The mission was adversely impacted by an inadequate approach to C2 that suffered from compartmentalization and evidenced mutual distrust between and among these service components. There was also a lack of unified command, with no single component commander to unify the Air Force airplanes and Navy helicopters, and no single ground commander to unify Delta Force and the Rangers. These organizational problems were exacerbated by the fact that the organizational units used different communications equipment that was not always interoperable.

Not all mishaps of the type described above are preventable with better technology, or with the fundamental scientific research that may one day lead to such technology. The point of the above example is that it shows the potential catastrophic effects of communications and coordination failures--and *some* such failures may indeed be preventable in the future if the right fundamental research is done today.

2.3 The Mission Value Pyramid

The observations above, and previous studies[7], suggest a simplified model of what is necessary for a successful enterprise approach. Mission or enterprise success relies on communication of the right information to the right actors at the right time. This in turn relies on an appropriate willingness and predisposition to communicate, which depends on organizational factors such as trust, and choosing an organizational structure and enterprise approach suited to the mission at hand. Finally, the behavioral willingness and predisposition to communicate must be undergirded by an ability to communicate, with an assured communications technology supported by proper policy, planning, and provisioning.

The "Mission Value Pyramid of Figure 1 codifies and graphically depicts these notions. Mission success relies crucially on adopting the appropriate enterprise approach. The appropriate C2/enterprise approach must be supported by effective composite networks comprising communications, information, and sensor capabilities. These composite networks must be effectively managed, and must consist of effective, efficient and agile component networks. All this in turn relies on a bedrock of assured communications capability.

[7] Vassiliou et al. (2015); Alberts (2011)

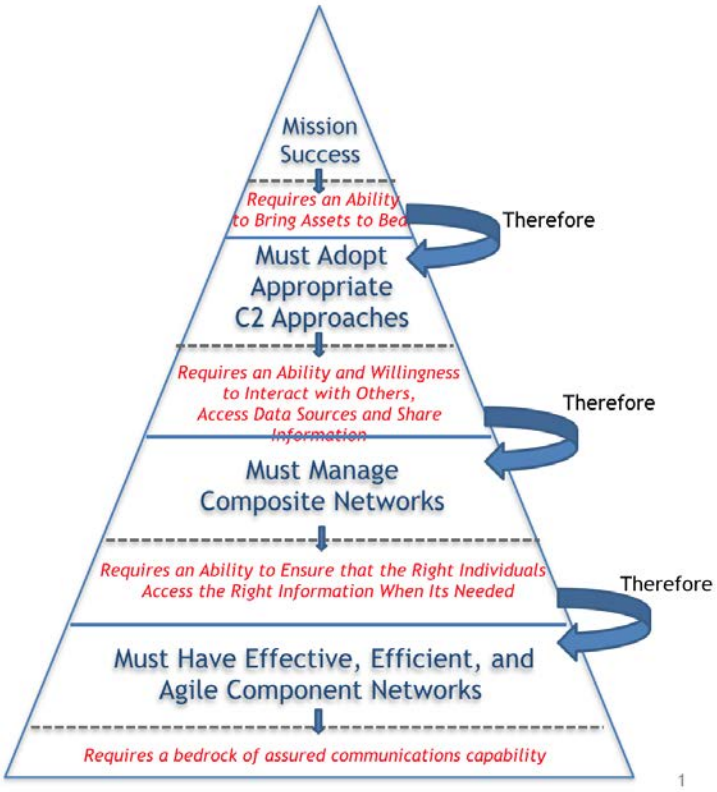

Figure 1: The Mission Value Pyramid

Mission partners are crucial for mission success, but they also complicate the adoption of an appropriate C2/enterprise approach, and increase the complexity and difficulty of managing composite networks. The adoption of an appropriate C2/enterprise approach is constrained by the mission environment, which also challenges and stresses the component networks. This is shown in Figure 2.

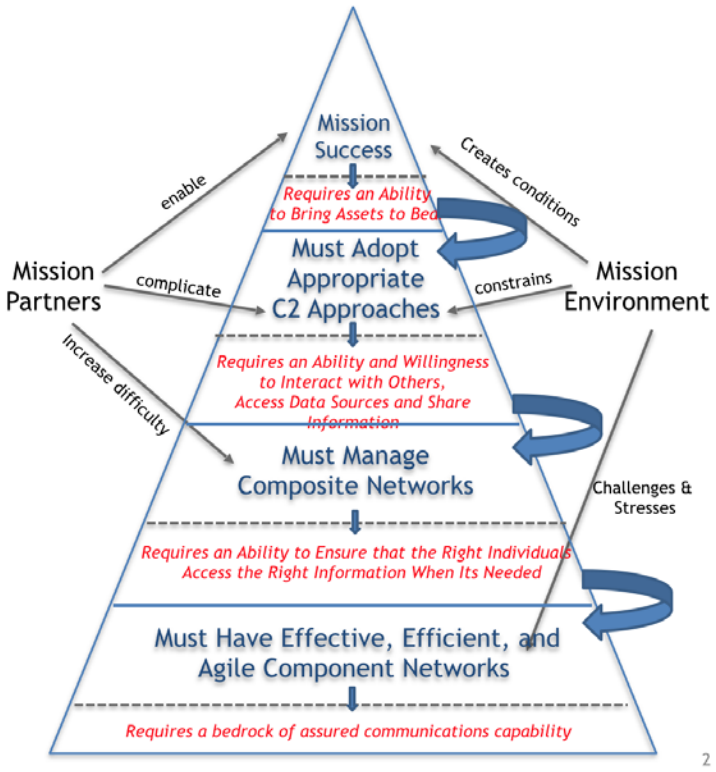

Figure 2: The Mission Value Pyramid with Conditions and Constraints

The likelihood that key information will be communicated to those who need it in a given mission can be increased by adopting the appropriate enterprise approach for that mission,[8] as shown in Figure 3. Studies of enterprise approaches in both military and civilian contexts have categorized such approaches according to the following, partially interdependent dimensions[9]:

- Allocation of decision rights. Are decision rights broadly distributed among actors, or are they more concentrated in a central authority?
- Information Distribution: is information broadly disseminated or guarded more closely by certain key actors?
- Patterns of Interaction. Who can talk to whom? Are interactions strictly and narrowly prescribed or are they broader?

[8] Alberts and Vassiliou (2015)
[9] Alberts and Hayes (2006); Alberts et al. (2010)

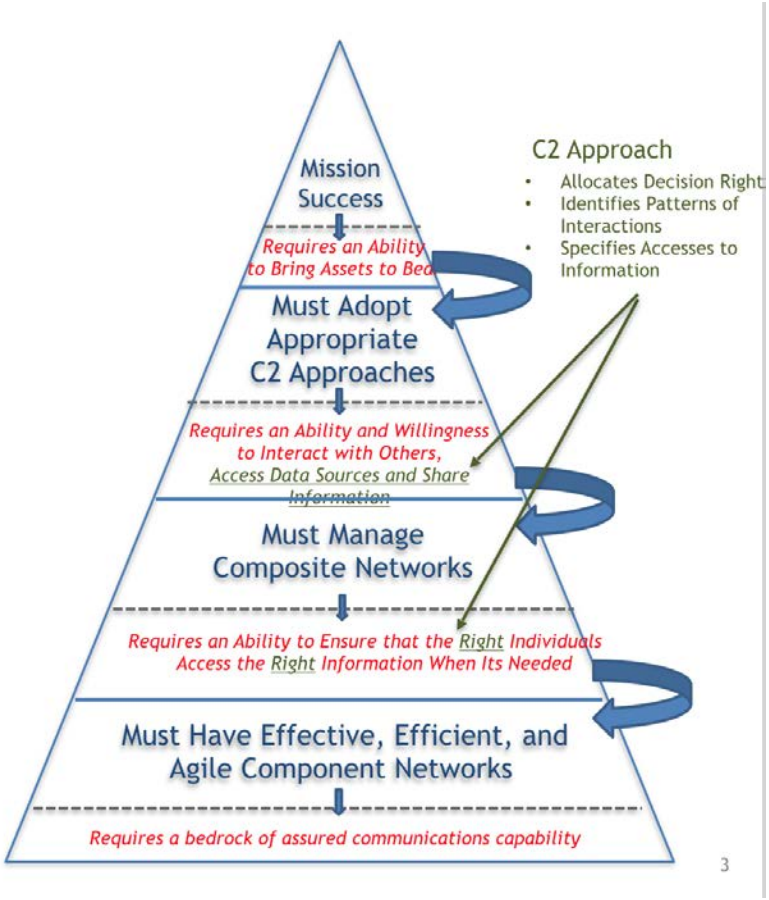

Figure 3: Impact of C2 Approach (Enterprise Approach) on the Mission Value Pyramid

3. Basic Research Directions: Examples

Every block in the Mission Value Pyramid suggests and requires fundamental research, as shown in Figures 4 and 7. Below we discuss a few of the possible directions of fundamental research.

3.1 Lowest Levels of the Mission Value Pyramid: Assured Communications and Component Networks

We may characterize an assured communications system as possessing three overarching facets: Agility, Protection, and Resilience. An agile system is one that is able to reconfigure dynamically to manage links and data across spectral bands, channels, and waveforms. A protected system is one that can overcome adversarial attacks or tampering. A resilient system is one that is able to tolerate faults and disruptions. Agility and protection both also enhance resilience: an agile system can, for example, avoid disruption in one band by moving to others; and a protected system can help prevent a large class of faults that adversaries are trying to induce.

There are a number of basic research advances that will be necessary. The topics discussed below, shown also on Figure 4, are examples.

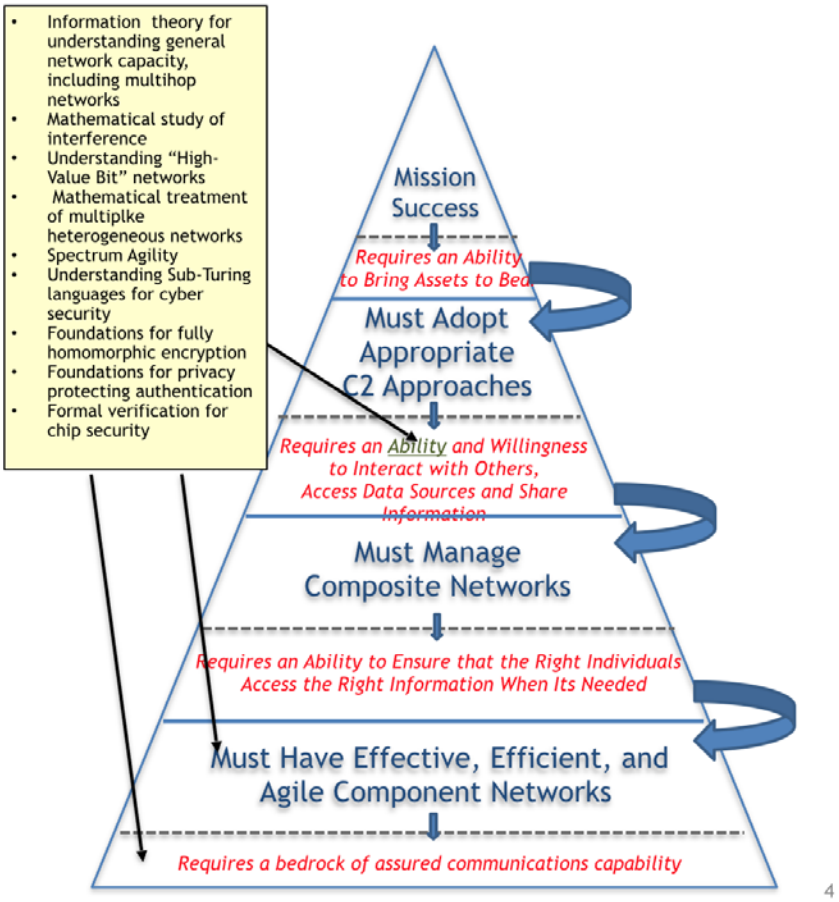

Figure 4. Basic Research Directions supporting lower levels of the pyramid: Assured Communications and Effective Component Networks

3.1.1 Information Theory for General Network Capacity

In order to provide effective communications capability, it is crucial to understand the theoretically possible information throughput of a system. For a single wireless link, this has been possible since the late 1940s, when Shannon (1949) published his seminal paper showing that the capacity of a link with a Gaussian noise channel is given by $C = B\log_2(1 + SNR)$, where B is the bandwidth, and SNR is the signal-to-noise ratio. This formula and the theory behind it have allowed performance to be predicted accurately enough to inform the design process, and in more recent times we have seen the buildup of a massive and effective commercial communications capability where wireless users are generally a single hop away from a wired infrastructure.

While the ability to understand communications capability over one link is thus relatively mature, the ability to do so simultaneously to a collection of users over a network, particularly a mobile ad-hoc wireless network, is far less so. When it comes to multi-hop wireless links, we are

essentially where the world was for one-hop wireless in 1948, before Shannon theory. This is illustrated in Figure 5.

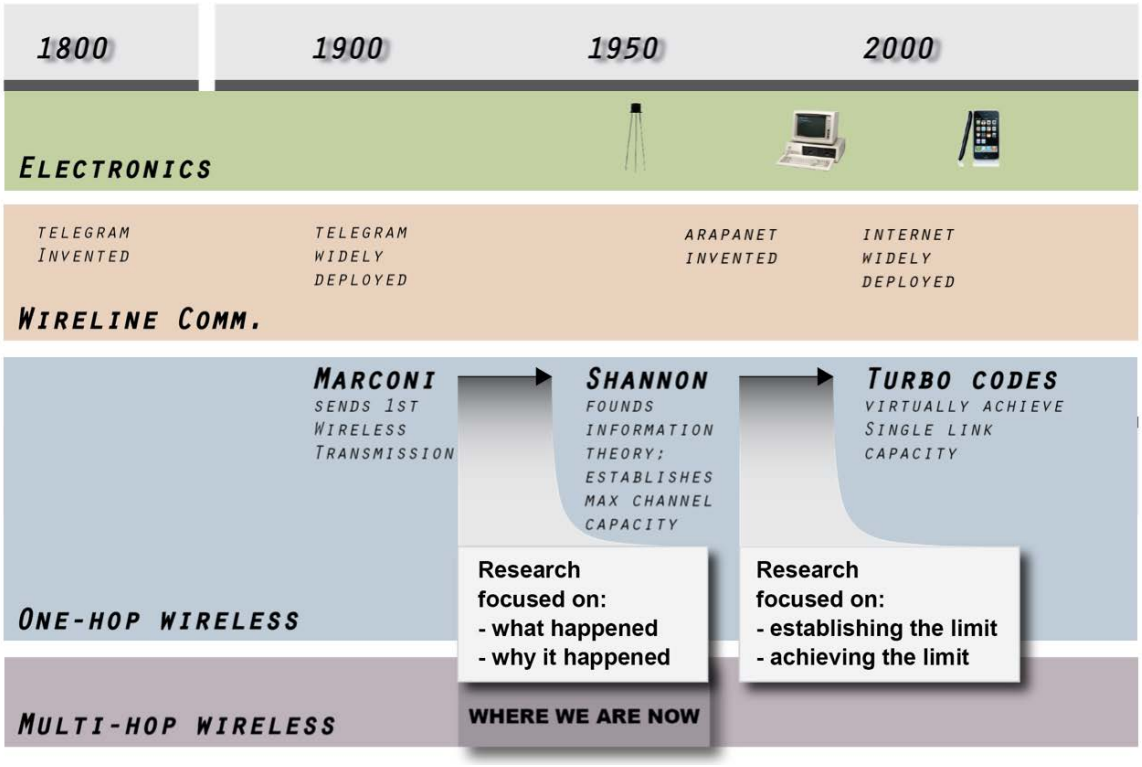

Figure 5. (From MacDonald et al., 2012) Wireless research timeline. For general multihop wireless networks, our level of theoretical development is roughly what it was for single-hop links in the 1940s.

Unfortunately, Shannon theory does not translate easy to multi-hop wireless networks. Andrews et al. (2008) have identified three fundamental roadblocks, which we summarize below in slightly different form:

1. Characterizing capacity of a mobile ad hoc wireless network requires fundamentally different assumptions that greatly complicate the approach. Compared to single wireless links, wireless networks have "bursty" traffic, and much higher delays driven by external dynamics.

2. General mobile ad-hoc wireless networks are difficult to decompose based only on links. Decomposition must take into account the varying interactions between nodes in space and time. Thus it is difficult to apply Shannon-like theory to individual links and characterize the system as an aggregation of those links.

3. In general mobile ad-hoc wireless networks, overhead is a high enough burden that it must be accounted for in the capacity theory itself.

Attacking the network capacity problem will require continued intensive research in fundamental information theory.

A related direction of information-theoretic research is to develop a better understanding of the scalability of networks, particularly mobile ad hoc wireless networks. Gupta and Kumar (2000) published a fundamental paper on the scalability limits of such networks. This type of work should be expanded, particularly taking into account different types of physical layers. In addition, mathematical explorations into the effect of various measures that might mitigate scalability problems (for example, the use of directional antennas[10]) are desirable.

3.1.2 Mathematical study of interference

Communications science can benefit from a more comprehensive theoretical treatment of interference, particularly interference that cannot be characterized as Gaussian. Strong interference in fact tends not to be Gaussian, leading to erroneous conclusions about reliability and capacity of communications systems and networks. Interference can often be cast as shot noise. This characterization can be particularly effective if there is a good statistical way to model the positions of the interferers. The field of stochastic geometry provides some of the necessary tools[11], and further research into the fundamentals of this field is warranted. The mathematics of purposeful interference alignment, to enable higher communication density, should also be further studied.[12]

3.1.3 Understanding "High-value-bit" networks

In command and control situations, reliable delivery of a very small amount of information—even a simple "yes" or "no"—can be more important than all the high-bandwidth video in the world. If there are a few high-value bits and many transmitters, random access of transmitters to channels becomes important, and this raises a number of information-theoretic issues. For example, what is the optimal transmission strategy? One is to embed high-value bits in the actual request for access. We do not yet have the theory to enable us to do that optimally, especially with heterogeneous transmitters of varying power.

3.1.4 Mathematical treatment of multiple heterogeneous networks

Commercial networks (and most DoD acquisition efforts) have tended to be homogeneous. They have tended to solve problems within their boundaries and have often had very strict control on the equipment in the network. Homogeneity greatly simplifies many networking challenges. Recently, the commercial world has begun to consider explicitly heterogeneous networks involving coexistence of a range of different radio access technologies and Wi-Fi, as well as cells of varying sizes[13]. However, the military is planning much more complex heterogeneous deployments, to connect various echelons of ground units to themselves and one another, as well as to airborne networks and satellites in orbit.

[10] Davis et al. (2006)
[11] Chiu et al. (2015); Elsawy et al. (2013); Wu et al. (2016)
[12] E.g., Tresch and Guillaud (2010)
[13] Nokia Siemens Networks (2011)

The protocols used to connect users within a network are often different than the protocols used to connect different networks together. This is true in the wired Internet today, but the vast majority of research on mobile networks to date has focused on protocols for connecting within networks, so there is a need and an opportunity for research into protocols that connect different networks, particularly in dynamic environments. For connections within a network in static environments, there are mature protocols such as Open Shortest Path First (OSPF), based on Dijkstra's algorithm[14]. For connections across networks in a static environment, there are protocols such as Border Gateway Protocol (BGP).[15] The large body of research into Mobile Ad Hoc Networks (MANETs) [16] has focused on intra-network connections in a dynamic environment. An opportunity for potentially useful research exists in the case of internetwork connections in dynamic environments. This is depicted in Figure 6.

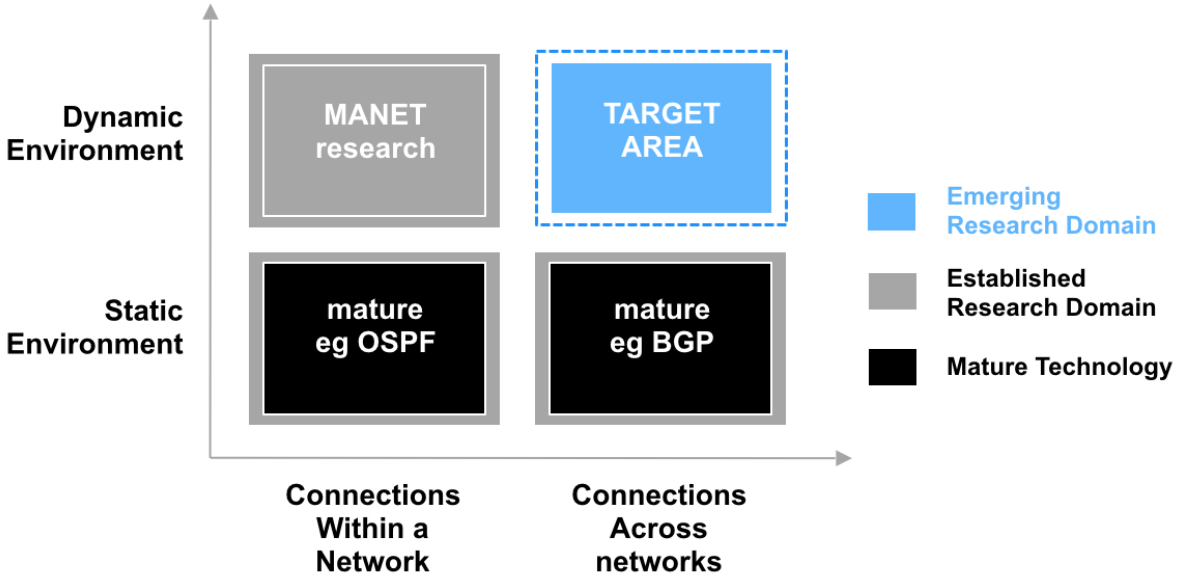

Figure 6. (From MacDonald et al., 2012) Emerging research domain in internetwork connection.

In more fully understanding internetwork connections and their behavior, we may also need to consider the explicit application of different metrics, including reliability and security, rather than focusing only on optimal routing and speed of delivery. New metrics may require new basic mathematics.

3.1.5 Spectrum Agility

Communications systems will need to be increasingly agile across spectral bands, for reasons not only of security, but also efficiency. Radio Frequency (RF) spectrum is a precious resource of

[14] Dijkstra (1959); Moy (1998); Tadimety (2015)
[15] Rekhter et al. (2006)
[16] Basagni et al. (2013)

increasing scarcity. Between 1992 and 2010 in the U.S., the Federal Government agreed to give up access to 412.5 Megahertz of spectrum, significantly impacting the Department of Defense. The most recent U.S. auction, for Advanced Wireless Systems-3 (AWS-3) in the 1695-1710 MHz, 1755-1780 MHz, and 2155-2180 MHz bands, netted about $41.3B,[17] suggesting an average value of nearly US$2 per Megahertz per person.

Many of the technological advances that will be necessary for dynamic spectrum management and sharing fall in the category of applied research and advanced engineering, rather than fundamental research: such advances include small cell technology, smart antennas, and RF design for agility. Effectively exploiting the millimeter wave band will require some fundamental advances in the efficiency of power amplifiers, which can now be as low as 8% in that band.[18] We will not discuss this in detail here because this involves semiconductor-related research outside the focus of this paper.

One area related to spectrum agility that can benefit from additional fundamental research is the creation of truly intelligent cognitive radios that can automatically and seamlessly share spectrum, and optimize their transmission parameters.[19] This will require research into cognitive engines, allowing radios to adjust parameters in order to identify and manage available spectrum, and even anticipate "holes" before they occur. Cognitive radios may incorporate database management techniques for dynamic spectrum access and sharing. How these databases are stored, accessed, and maintained may constitute an important set of research issues. Should the databases be distributed or centralized? How can sensitive information about, for example, the operation of a radar system which is sharing spectrum with communications systems, be kept secure? Information-assurance and privacy will be crucial issues when spectrum is shared.

3.1.6 Cyber Security: Sub-Turing Languages

The problem of assuring security in the face of cyber-attack is an extremely difficult one. Simply put, there is a fundamental asymmetry involved: looking for ways to attack a system is much easier and cheaper than anticipating all the attacks and guarding against them, let alone proving that one has done so. Some investigators have gone as far as to say that, when computers using general purpose processors and languages are connected to each other, cyber-security is provably impossible.[20] Programs written in general purpose languages, operating on general purpose processors, have an immense amount of computational privilege, perhaps more than they need. The privilege may lie unused until an attacker discovers it and exploits it.[21] One approach may be to restrict the capability space of computers. Doing so in a way that makes sense, and still allows the computers to fulfill their useful purposes efficiently, will require fundamental research in formal computation theory and languages.

---

[17] FCC, "Auction of Advanced Wireless Services (AWS-3) Licenses Closes, Winning Bidders Announced for Auction 97," Washington, D.C., United States Federal Communications Commission Public Notice DA 15-31, January 30, 2015. https://www.fcc.gov/document/auction-97-aws-3-winning-bidders

[18] Reed et al. (2016)

[19] Reed et al. (2016)

[20] Mitola (2016)

[21] Bratus et al. (2014)

An example of a promising research area is that of "Sub-Turing languages." Programming languages have generally striven to be Turing-Complete[22], in order to afford the programmer a maximum of usefulness and flexibility. However, Turing completeness can lead to state-space explosion that makes it difficult or impossible to conduct formal verification of the security of inputs and analyze the termination properties of large programs. Are Turing-Complete languages more powerful than needed?[23] A sub-Turing language can mitigate or avoid some of the aforementioned problems by, for example, limiting the transition function so that the underlying conceptual Turing Machine cannot return to a previously visited state. This can guard against indefinite non-termination. Some good exploratory research has already been done in this area.[24] Much more is needed, for example, to fully explore the theoretical tradeoffs between provable security and computational power and flexibility.

3.1.7 Fully Homomorphic Encryption

Conventional encryption suffers from the property that, once data is encrypted, it needs to be decrypted in order to be processed. A highly desirable form of encryption—fully homomorphic encryption (FHE)—allows data to be processed while still in its encrypted state.[25] This enables, for example, search queries to be sent to a server in encrypted form, with the results returned in encrypted form and the server never knowing what the query was. [26] It also makes possible a wide variety of other blind server-side computations. The problem of creating this type of encryption was posed by Rivest et al. in 1978. For a long time it remained a highly desirable but unattained goal, but this changed with a breakthrough by Gentry (2009a,b), who presented the first fully functional scheme for FHE.

FHE should now be the subject of continuing, intensive fundamental research. It is still far too slow to be generally useful: encryption of a single bit takes more than a second on a high-end Intel Xeon based server.[27] Some schemes have recently been published on hardware acceleration of FHE.[28] More fundamental theoretical work will also be required to discover ways to speed it up. Theoretical work should also be done on languages and compilers used to implement FHE.

3.1.8 Privacy-Protecting Authentication

"Authentication" refers to the technology, systems, and procedures that enable senders to prove their identity to receivers, and allow receivers to feel confident that the senders were the true originators of the communications in question. In some cases, it may be desirable for the sender to be authenticated and remain anonymous. In those cases, what is desired is "privacy-protecting

[22] A language is Turing-Complete, or Turing-Equivalent, if it can be used to simulate any single-taped Turing Machine.
[23] Sassaman et. al. (2013).
[24] Reilly et al. (2015)
[25] Micciancio (2010)
[26] Ramyal and Saravanan (2016).
[27] Wang et al. (2015)
[28] Ozturk et al. (2017)

authentication" (PPA). Such applications include device-to-device communications in the Internet-of-Things (IoT), among many others.

Approaches to PPA fall into two general classes, pseudonym based signatures[29], and group signatures[30]. Pseudonym based approaches can use existing public-key cryptography. They suffer from large burdens associated with key management and distribution. Group signature approaches do not require public-key certificates, and thus avoid that overhead. In such schemes, each signer is a member of a group, and is issued a private key tuple by the group manager. The private key tuple enables signatures from which the signer's identity cannot be deduced by receivers, but can be revealed by the group manager in case of conflict. Many such group-based PPA schemes have been introduced. Relevant mathematical foundations include bilinear pairings[31] and elliptic curve cryptography[32]. These are fields worthy of further investment in basic research.

3.1.9 Formal Verification for Chip Security

Computer and communications security has generally focused on software, with a prevailing assumption that the microchips running the software are secure. Yang et al. (2016) presented an ingenious attack method on microchips that calls this assumption into question.[33] The attack is analog in nature, and thus avoids the usual digital triggers that alert diagnostic systems that something has gone wrong. It is based on inserting a single component, among hundreds of millions, into the chip design before fabrication. The component acts as a capacitor, building up charge until it reaches a threshold and then triggering a takeover of the operating system. The capacitor's activity is not detected because it builds up voltage at levels between those associated with a digital "0" and a digital "1." Although this type of attack requires access to the chip design and fabrication process, it nevertheless raises a significant alarm. Basic research will be needed into formal verification methods that include risks from analog circuits interacting with digital ones at levels below the surveillance span of current detection schemes.

3.2 Higher Levels of the Mission Value Pyramid

To address the needs of the higher levels of the Mission Value Pyramid, basic research may be necessary that blends mathematical, physical, and social sciences. Below we discuss some selected topics, shown also on Figure 7.

[29] Kumar et al. (2015)
[30] Boneh and Shacham (2004)
[31] Boneh and Franklin (2001); Islam and Biswas (2012)
[32] Miller (1985); Koblitz (1987); Islam and Biswas (2011).
[33] See Greengard (2017) for a concise description; Yang et al. (2016); Wahby et al.(2016)

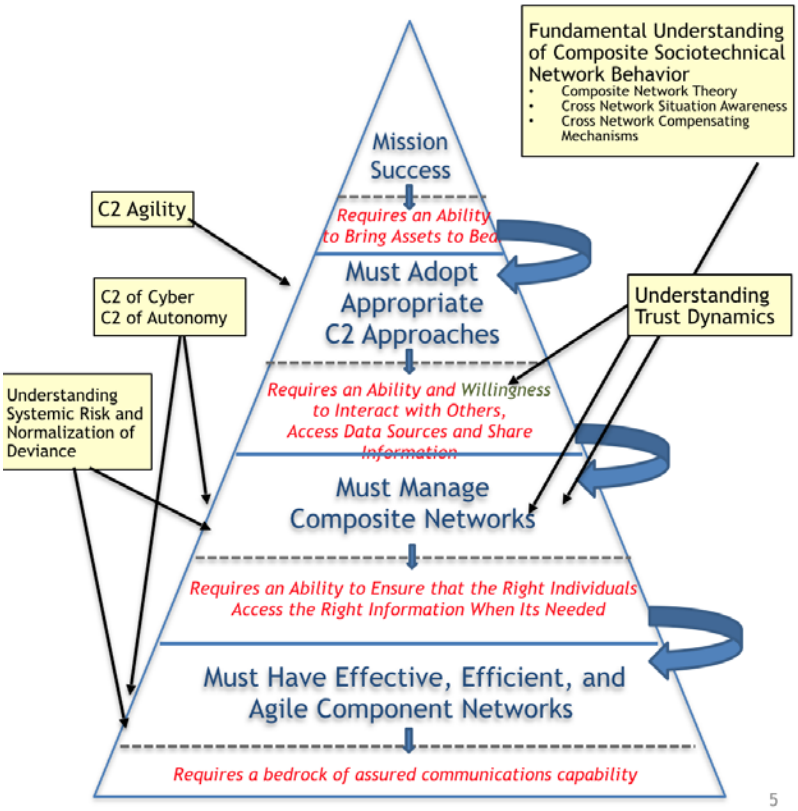

Figure 7. Basic Research Directions supporting higher levels of the Mission Value Pyramid

3.2.1 Understanding Composite Networks

The term "Composite Network" refers to the set of heterogeneous, inter-dependent multi-genre networks that enable complex endeavors such as military missions.[34] A notional global view of a composite network is shown in Figure 8. Composite networks may include communications, information, sensor, and command-and-control networks. Note that networks of each of these genres may themselves be heterogeneous assemblages of multiple networks, as discussed above. While many single genres of networks have received considerable research attention over the years, the cross-genre 'connections', interactions and interdependencies that give purpose to these networks and shape and constrain their individual and collective behaviors have not been adequately investigated.

[34] Alberts et al. (2015)

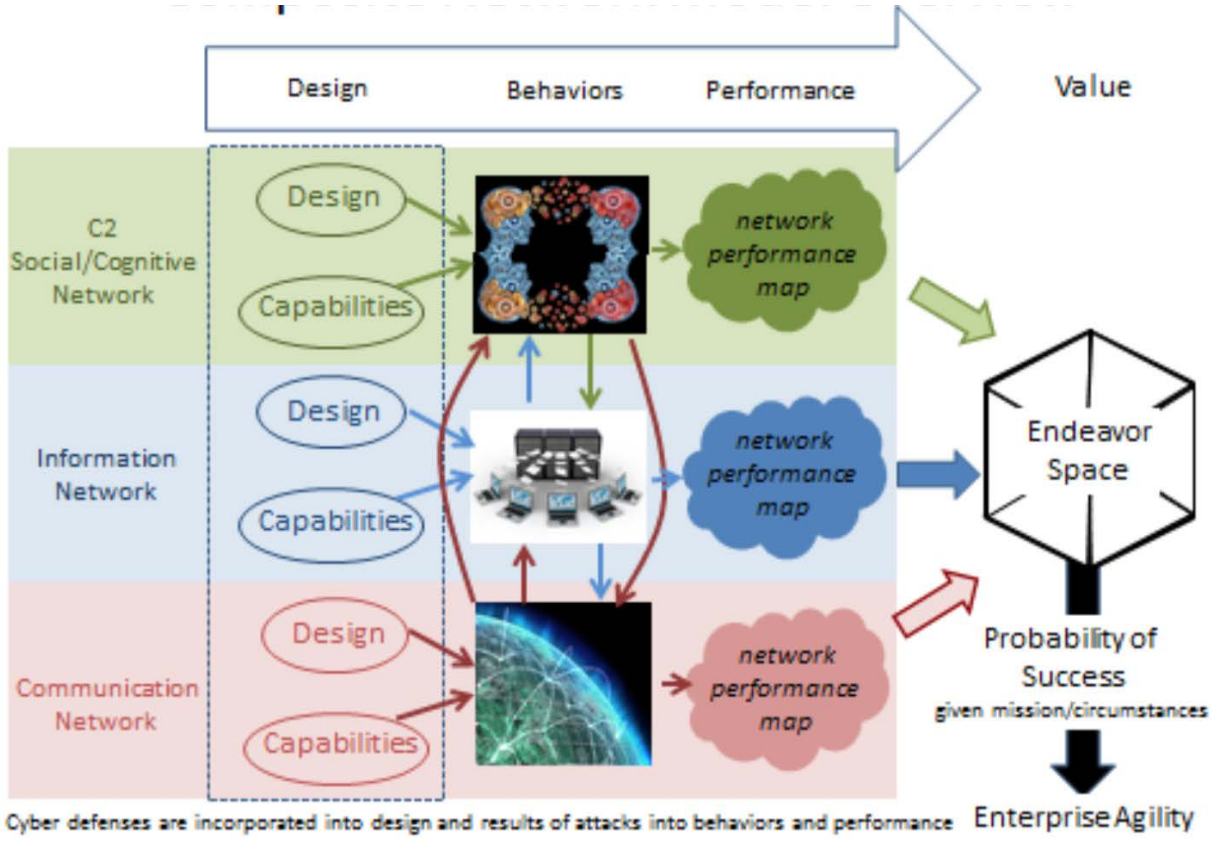

Figure 8. (From Alberts et al., 2015), A composite network, comprising several genres of networks. Each genre may be complex. The communications network, for example, may be composed of multiple heterogeneous networks.

The objective of achieving a better understanding of composite networks, their component entities, their interactions, and their behaviors is to improve our ability to create both composite and component network designs and employ smart and agile mechanisms that mitigate the risks of undesirable behaviors and outcomes that would otherwise adversely impact individual and composite network performance and mission effectiveness.

Achieving this research objective is made considerably more challenging for a number of reasons. First, the networks and entities of interest do not exist in isolation from one another; rather they interact with and are dependent upon one another to achieve their various individual purposes. Furthermore, it is their collective behavior (composite network behavior) not only their individual behaviors, that determine their fitness for purpose. This means that one must understand and consider design and performance tradeoffs from a composite network perspective.

Second, complex endeavors, such as many military ones, take place in highly dynamic, contested environments. Therefore, it is inevitable that the entities that are the subjects of this research will be destroyed, damaged, disrupted, and/or compromised. This, in turn, will affect their behaviors

in ways that impact not only their ability to function but also their ability to support other entities, in the same or a different genre, as required.

Achieving an understanding of composite networks will require interdisciplinary research spanning applied mathematics, computer science, communications, and psychology. New simulation methods will need to be developed, as well as new ways to instrument the real world to collect and analyze the necessary data about interactions, cooperation, etc.

3.2.2 Understanding Composite Network Agility

Agility is increasingly being recognized as a crucial attribute for individuals, organizations, and the systems that support them as enterprises are called upon to succeed in environments that are increasingly complex and dynamic.[35] Agility is the capability to successfully cope with, and exploit, unexpected circumstances and changes in circumstances, and to rapidly reconfigure one's enterprise/C2 approach and concomitant execution. A major research challenge is the formulation of endeavor spaces [36] for individual and composite networks that capture unexpected circumstances and changes in circumstances.

Commanders and managers at all levels are faced with the challenge of assuring that their organizations and endeavors will be agile enough while network and system designers and developers will need to ensure that networks and systems can adequately support users under these conditions. The state of the art of agility measurement is currently limited to measures of manifest agility, that is, observations that recognize whether or not an entity has exhibited a requisite amount of agility in a specific situation.[37] To understand how to judge if an entity has the agility it will need to face an uncertain future, research is needed to be able to better answer the following three questions.

- How can one measure *potential* agility?
- What is the required amount of agility?
- How can potential agility be designed and incorporated?

3.2.3 Understanding Agile Network Compensating Mechanisms

The ability to reconfigure the C2 or enterprise approach to suit changing circumstances is called "C2 Maneuver." C2 Maneuver is, in effect, an agile network compensating mechanism for the organizational component of a composite C2 network. It represents human and organizational adaptation to circumstances and conditions. Some of these changes will be related to a change in the state of one or more of the other networks in the composite network that impact the ability of

[35] Vassiliou et al. (2015); Alberts (2011)

[36] Alberts et al. (2011) define an Endeavor Space as "a multi-dimensional space that includes the set of conditions and circumstances that could impact composite network and mission performance. Endeavor Space dimensions are associated with specific characteristics of the mission, the environment, and the states of the relevant entities and actors. Each region of this space provides a specific mission context and specifies the conditions of interest that can impact network behaviors, measures of performance (MoPs) and measures of effectiveness (MoEs)."

[37] Alberts (2011); NATO (2013)

the C2 nodes to continue to function. For example, disrupted communications may prevent a node from properly exercising decision rights (lack of information or lack of connectivity to issue orders). In order for the C2 Composite Network to function appropriately, decision rights may need to be reallocated.

Degraded communications in general are an important stressor of a composite network. They may result from a number of causes, such as environmental conditions that affect the transmission of signals, or spikes in workload created by humans. One can conceive of agile network compensating mechanisms that could be embedded in communications and/or information networks that are able to recognize the situation and adapt.

Agile network compensating mechanisms require the ability to make informed decisions that, in turn require, the following: a knowledge of one's own state and the states of the networks that are impacting or are impacted by the network; an understanding of adaptation options; and, a mapping of states to appropriate options.

To satisfy these requirements, new research is needed on:

- How component networks need to be instrumented, and how the instrumentation can be accomplished.
- How component network state data can be used to create action-oriented "dash boards" for internal and external consumption
- Understanding the range of network adaptation options, and
- Mappings of states to options

3.2.4 C2 of Composite Networks and Cyber

Purposeful networks need to be managed to ensure adequate effectiveness while balancing efficiency and risk. Among the risks is the presence of persistent cyber-attacks that can impact, in different ways, each of the networks in a composite network. Defending against cyber-attacks involves both dynamic countermeasures and mitigations that involve multiple network genres. These defenses and mitigations are instances of compensating mechanisms that need to be understood in the context of purposeful composite networks. Other compensating mechanisms will be required to cope with a variety of other stresses.

Designing and building compensating mechanisms into each of the component networks, will collectively create a capability for network co-adaptation that could dramatically increase composite network agility. However, with dynamic co-adaptation comes added complexity that will need to be understood and managed. In other words, we need the ability to perform C2 on C2 itself—that is, command and control of composite networks including C2 networks, and C2 of Cyber.

C2 of composite networks involves dynamically setting the available component network parameters to achieve a desired effect. These parameters include but are not limited to the C2

Approach of the C2 network *within* the composite network, user access controls, information sharing policies and practices, message priorities, and routing.

A major research challenge is to understand the nature of the tradeoffs between and among component network performance, cyber defense and countermeasures, and overall Composite Network performance as well as the cross network connection topology necessary to dynamically change the values of the parameters of interest.

3.2.5 Understanding Trust Dynamics

Trust, or a lack thereof, plays an important role in human behavior[38] that, in turn, shapes and constrains composite network behaviors and performance. A lack of trust can freeze information in place, while appropriate trust assessments can move the right information along to the right places.

There are many forms of trust that come into play. These include trust in information sources, in pieces of information, in leadership, subordinates, and organizations, and in systems that impact information seeking, information sharing, perceptions, decision-making, and collaboration.[39]

Trust levels are established and influenced by a host of factors including education, training, experience, team hardness, and culture. Cyber-attacks can adversely impact trust levels across the board and thus network behaviors. Research questions abound:

- What are the important instantiations of trust (e.g. trust in information sources, etc.)?
- How can the various levels of trust be measured and monitored?
- How much trust is required for composite networks to function successfully?
- How can levels of trust be increased?
- What network compensating mechanisms can be used to mitigate the effects associated with low or falling trust levels?
- How can we determine if substantial investments in cybersecurity/mitigations are justified by the avoidance of the trust-related costs they create?

New, fundamental research is required to elucidate how individuals and groups form trust assessments, and how they act in light of these assessments. Understanding these dimensions of trust will help us determine how to make appropriate evaluations of trust, and how to act accordingly in C2 systems. Learning the consequences of given levels of trust on the information sharing dynamics of networked entities will help us select the most effective approach to C2 based on trust levels. It is also important to develop an understanding of how trust is built, and if that process can be accelerated in distributed environments. Similarly, it is important to understand

[38] E.g., Mayer, Davis & Schoorman, (1995)
[39] Hieb (2015)

how trust can be degraded, in order to protect against such degradation, or to visit degradation upon an adversary.

3.2.6 Understanding Systemic Risk

Large-scale, complex systems are often robust to idiosyncratic shocks and component failures, yet under certain circumstances, these shocks aggregate and have systemic effects.[40] The great recession of 2008, and the power outage of 2003 are examples.[41] Furthermore, we do not yet understand how to monitor systems to be able to predict when such failures happen. What measurements should be made? What kind of data need to be gathered?

3.2.7 Normalization of Deviance: Game Theory

Related to the problem of understanding systemic risk is understanding the phenomenon of normalization of deviance.[42] This is illustrated by the observation that if a hundred people are all watching your child, then no one is watching your child: effectively, each person assumes the others are watching. People make internal and even unconscious calculations of the low probability of failure if they are not vigilant, assuming that everyone else is vigilant. If everyone does this and acts accordingly, there can be a catastrophic failure. Normalization of deviance has been identified as at least a partial causative mechanism in a host of disasters, including the Challenger Disaster, the Union Carbide Bhopal tragedy, and the nuclear accident at Three Mile Island[43]. It is a phenomenon that may also operate in various ways and at various levels in the composite networks that will be necessary for future mission success.

Benoit and Dubra (2013) identify two factors leading to a lack of proper preventive care. These are, quoting directly from the paper:

> "(1) When objective risks of a disaster are poorly understood, positive experiences may lead agents to underestimate these risks and underinvest in preventative care.
>
> (2) Redundancies designed for safety may induce agents to lessen the care they take."

Thus, a system may become less safe even as it appears to be getting safer. Measures designed to reduce overall system risk can in fact increase that risk. Benoit and Dubra present a game-theoretic model for normalization of deviance, and conduct a rigorous analysis. Additional fundamental research along these lines is desirable, to develop a fuller understanding of this important phenomenon.

[40] The wording of this section is closely paraphrased from material supplied by VBFF fellow Professor Ali Jadbabaie of MIT

[41] Acemoglu et al. (2015)

[42] Gunn and Gullickson (2004)

[43] Benoit and Dubra (2013)

4. Concluding Remarks

In this paper we have outlined a conceptual framework for the ingredients of success in complex missions--the “Mission Value Pyramid”--and used that framework to motivate and suggest some example areas of fundamental research that have the potential to contribute ultimately to those ingredients.

We have considered topics in applied mathematics, information theory, computer science, and emerging disciplines such as sociotechnical network theory that may involve social sciences and psychology as well.

At lower levels of the Mission Value Pyramid, concerned with assured communications, some of the areas we identify include information theory for general, multi-hop, wireless mobile networks; mathematical treatment of multiple heterogeneous networks and their interconnection protocols; sub-Turing languages for cyber security; and new mathematics with applicability to encryption. At higher levels of the Pyramid, important areas include achieving a fundamental understanding of the behavior of composite networks, including trust dynamics. The understanding of systemic risk, and phenomena such as the normalization of deviance, are also important.

The areas outlined above do not constitute an exhaustive set, and many others are possible and desirable. We have, for example, not yet touched on the important fields of data science and data analytics. However, the topics we have considered all require fundamental research, and all have the potential to make a significant positive impact on command, control, and communications.

Acknowledgement and Disclaimer

This work was conducted by the Institute for Defense Analyses (IDA) under contract HQ0034-14-D-0001, Task AI-2-3771. The views, opinions, and findings should not be construed as representing the official position of the United States Government or any of its agencies. This paper was approved for public release; distribution is unlimited.

References

Acemoglu, Daron, Asuman Ozdaglar, and Alireza Tahbaz-Salehi (2015). "Systemic Risk and Stability in Financial Networks." American Economic Review 2015, Vol. 105, No. 2, 564–608.

Alberts, David S. (2011). "The Agility Advantage." Washington, D.C.: United States Department of Defense, Command and Control Research Program (CCRP Press), 615pp.

Alberts, David S., and Richard E. Hayes (2006). Understanding Command and Control. Washington, D.C.: United States Department of Defense, Command and Control Research Program (CCRP Press), 255ppt

Alberts, David S., Reiner K. Huber, and James Moffat (2010). NATO NEC C2 Maturity Model. Washington, D.C.: United States Department of Defense, Command and Control Research Program (CCRP Press), 365pp.

Alberts, David, Alexander Kott, Brian Rivera, Kevin Chan, Lisa Scott, Reginald Hobbs, Alice Leung, Will Dron, and Ritu Chadha (2015). Network Science Experimentation Vision. Adelphi, Maryland: United States Army Research Laboratory, Report No. ARL-TR-7451

Alberts, D. S., and M. S. Vassiliou (2015). "The Quest for Key Information: Does C2 Approach Matter?" Proc. 20th International Command and Control Research and Technology Symposium.

Andrews, Jefffrey, Sanjay Shakkottai, Robert Heath, Nihar Jindal, Martin Haenggi, Randy Berry, Dongning Guo, Michael Neely, Steven Weber, Syed Jaffar, and Aylin Yener (2008). "Rethinking Information Theory for Mobile Ad Hoc Networks." IEEE Communications Magazine, Dec. 2008, 94-101.

Anno, Stephen E., and William E. Einspahr (1988). Command and Control and Communications Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid. Air War College Research Report No. AU-AWC-88-043. Maxwell Air Force Base, Alabama: Air War College.

Basagni, Stefano, Marco Conti, Silvia Giordano, and Ivan Stojmenovic (2013). Mobile Ad Hoc Networking:The Cutting Edge Directions. New York: Wiley/IEEE.

Benoît, Jean-Pierre, and Juan Dubra (2013). "On the Problem of Prevention." International Economic Review, Vol. 54, No. 3, 787-805.

Boneh, D., and Franklin, M. K. (2001). "Identity-based encryption from the Weil pairing." Proceedings of Crypto '01. New York: Springer, Lecture Notes in Computer Science 2139, 213-229.

Boneh, D. and H. Shacham (2004). Group signatures with verifier-local revocation. In Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS), 168-177.

Bowden, Mark (2006). “The Desert One Debacle.” The Atlantic Monthly, May, 2006, pp. 62-77.

Bratus, S., T. Darley, M. Locasto, M. L. Patterson, R. Shapiro and A. Shubina (2014). "Beyond Planted Bugs in ‘Trusting Trust’: The Input-Processing Frontier," IEEE Security & Privacy January/February 2014,. 83-87,.

Chiu, Sung Nok, Dietrich Stoyan, Wilfrid S. Kendall, and Joseph Mecke (2013). Stochastic Geometry and its Applications, 3rd Ed. New York: Wiley.

Davis, Chris, Zygmunt J. Haas, and Stuart D. Milner (2006). “On How to Circumvent the MANET Scalability Curse.” Proc. 2006 IEEE Military Communications Conference, 1-7.

Dijkstra, Edsger (1959). “A Note on Two Problems in Connexion with Graphs.” Numerische Mathematlk l, 269-271.

DoD (2016). Financial Management Regulation, DOD 7000.14-R, Vol. 2B, Ch. 5, p. 5-4. Washington, D.C.: Unites States Department of Defense.

ElSawy, Hesham, Ekram Hossain, and Martin Haenggi (2013). “Stochastic Geometry for Modeling, Analysis, and Design of Multi-Tier and Cognitive Cellular Wireless Networks: A Survey.” IEEE Communications Surveys 7 Tutorials, Vol. 15., No. 3, 996-1019.

Gentry, C. (2009a). Fully Homomorphic Encryption Scheme, Ph.D. dissertation, Department of Computer Science, Stanford Univ., Stanford, CA, USA.

Gentry,C. (2009b). “Fully Homomorphic encryption using ideal lattices.” Proc. Symp. Theory Comp., 2009, 169-178.

Greengard, Samuel (2017). “Are Computer Chips the New Security Threat?” Communications of the ACM, Vol. 60, No. 2, 18-20.

Gunn, Robert W., and Betsy Raskin Gullickson (2004). “The Normalization of Deviance.” Strategic Finance, March 2004, 1-3.

Gupta, Piyush and P. R. Kumar, "The capacity of wireless networks," IEEE Trans. Inform. Theory, vol. 46, no. 2, 388-404.

Hieb, Michael (2015). “Command and Control in Multiteam Systems: Measuring and Building Trust between People and Groups.” Proceedings of the 20th International Command and Control Research and Technology Symposium (ICCRTS).

Islam, S. H. and G. P. Biswas (2011). “Design of Improved Password Authentication and Update Scheme based on Elliptic Curve Cryptography.” Mathematical and Computer Modeling Vol. 57, No. 11, 2703-2717.

Islam, S. H. and G. P. Biswas (2012). “Certificateless Strong designated Verifier Multisignature Scheme Using Bilinear Pairings.” Proc. International Conference on Advances in Computing, Communications and Informatics ICACCI’12, 540-546.

Koblitz, N. (1987). “Elliptic Curve Cryptosystem.” J. Mathematics of Computation 48, 177, 203-209.

Kumar, Vireshwar, He Li, Jung-Min (Jerry) Park, Kaigui Bian, and Yaling Yang (2015). “Group Signatures with Probabilistic Revocation: A Computationally-Scalable Approach for Providing Privacy-Preserving Authentication.” Proceedings CCS '15: 22nd ACM SIGSAC Conference on Computer and Communications Security, 1334-1345.

MacDonald, Thomas, Carl Fossa, Matt Kercher, and Aradhana Narula-Tam (2015). Mobile Networking Research Challenges. Presented at the 17-19 July, 2012 Joint Tactical Edge Networking Meeting, held at MIT Lincoln Laboratories, Lexington, Massachusetts.

Micciancio, Daniele (2010). “A First Glimpse of Cryptography’s Holy Grail.” Communications of the ACM, Vol. 53, No. 3, 96.

Miller, V. S. (1985). Use of elliptic curves in cryptography. Proc. Crypto ’85. New York: Springer, 417-426.

Mitola, Joseph (2016). Autonomy in Contested Environments. Florida Institute on National Security Assured Autonomy Workshop, Fort Walton Beach, Florida, 5-6 April 2016.

Moy, J. (1998). OSPF Version 2. The Internet Society, Request for Comments RFC 2328.

NATO (2013). C2 Agility. Technical Report STO-TR-SAS-085. Brussels, Belgium: North Atlantic Treaty Organization.

Nokia Siemens Networks (2011). Designing, Operating, and Optimizing Unified Heterogeneous Networks. Espoo, Finland: Nokia Siemens Networks, 2011.

OECD (2002). Frascati Manual 2002: Proposed Standard Practice for Surveys on Research and Experimental Development. Paris: Organization for Economic Cooperation and Development.

Ozturk, Erdinc, Yarkin Doroz, Erkay Savas, and Berk Sunar (2017). “A Custom Accelerator for Homomorphic Encryption Applications.” IEEE Transactions on Computers, Vol. 66 No. 1, 3-16.

Ramyal, J. and M. Saravanan (2016). “Strengthening Encryption Secrecy for Private Search Using Fully Homomorphic Encryption.” ICTACT Journal on Communication Technology, Vol. 7, No. 1, 1255-1260.

Jeffrey Reed, Marius S. Vassiliou, and Syed Shah (2016), “The Role of New Technologies in Solving the Spectrum Shortage.” Proc. IEEE Vol. 104, No. 6, 1163-1168.

Reilly, Karen, Jacob Torrey, Jared Frank, and Trent Brunson (2015). CREMA. Rome, New York: United States Air Force Research Laboratory, Report No. AFRL-RI-RS-TR-2015-188.

Rekhter, Y., T. Li, and S. Hares (2006) (Eds.) A Border Gateway Protocol 4 (BGP-4). The Internet Society, Request For Comments RFC 4271.

R. L. Rivest, L. Adleman, and M. L. Dertouzos (1978). "On data banks and privacy homomorphisms." Found. Secure Comput., vol. 4, no. 11, 169-180.

Sassaman, Len, Meredith L. Patterson, Sergey Bratus, and Michael E. Locasto (2013). "Security Applications of Formal Language Theory," IEEE Systems Journal, Vol. 7, No. 3, 489-500.

Shannon, Claude (1949). "Communication in the Presence of Noise," Proceedings Institute of Radio Engineers, Vol. 37, pp. 10-21, 1949. Reprinted in D. Slepian, editor, Key Papers in the Development of Information Theory, IEEE Press, NY, 1974. Reprinted in Proceedings Institute of Electrical and Electronic Engineers, Vol. 72 (1984), pp. 1192-1201. Included in Part A.

Tadimety, Phani Raj (2015). OSPF: A Network Routing Protocol. New York: Apress.

Tresch, Roland, and Maxime Guillaud (2010). "Performance of Interference Alignment in Clustered Wireless Ad Hoc Networks." Proc. IEEE International Symposium on Information Theory, ISIT 2010, 1703-1707.

Vassiliou, M. S. and D. S. Alberts (2013), "C2 Failures: A Taxonomy and Analysis." Proc. 18th International Command and Control Research and Technology Symposium, Alexandria, Virginia.

Vassiliou, Marius, Jonathan R. Agre, Syed Shah, and Thomas MacDonald (2013). "Crucial Differences Between Commercial and Military Communications Technology Needs: Why the Military Still Needs its Own Research." Proc. IEEE Military Communications Conference MILCOM 13, 342-347

Vassiliou, M.S., D. S. Alberts, and J. R. Agre (2015), "C2 Re-Envisioned: The Future of the Enterprise." New York: CRC Press, 300pp.

Wahby, Riad S., Max Howald, Siddharth Garg, Abhi Shelat, and Michael Walfish (2016). "Verifiable ASICs." Proc. 2016 IEEE Symposium on Security and Privacy, 759-778.

Wang, Wei, Yin Hu, Lianmu Chen, Ximing Huang, and Berk Sunar (2015). "Exploring the Feasibility of Fully Homomorphic Encryption." IEEE Transactions on Computers, Vol. 64, No. 3, 698-706.

Wu, Liang, Yi Zhong, Wenyi Zhang, and Martin Haenggi (2016). "Scalable Transmission over Heterogeneous Network: A Stochastic Geometry Analysis." IEEE Transactions on Vehicular Technology, in press.

Yang, Kaiyuan, Matthew Hicks, Qing Dong, Todd Austin, and Dennis Sylvester (2016). “A2: An.alog Malicious Hardware.” Proc. 2016 IEEE Symposium on Security and Privacy, 18-37.