Strategy Research Project

Touch Points in Emerging Capabilities: Cyber, Space, and Special Operations

by

Colonel Mark E. Orwat
United States Army

United States Army War College
Class of 2014

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-04-2014	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
Touch Points in Emerging Capabilities: Cyber, Space, and Special Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Mark E. Orwat
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor William O. Waddell
Center for Strategic Leadership and Development

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 6,727

14. ABSTRACT

A key effort in developing Joint Force 2020 is to "pioneer new ways to combine and employ emergent capabilities such as cyber, Special Forces, and ISR" and "examine organizational and other force development changes to better leverage game-changing capabilities." Individually, the emerging capabilities are maturing in capability, capacity, and integration into military operations. However, collectively, the emerging capabilities are not advancing with respect to each other. This strategic research paper draws from my personal experience working in the three emergent areas and includes a comprehensive review of visionary concepts such as Joint Force 2020, SOCOM 2020, and LandCyber 2018-2030. Major touch points exist between emerging capabilities in terms of interoperable technology, organizational integration, and combined effects that will enable self-synchronization among networked cyber, space, and Special Operations Forces in support of the Joint Force. This research establishes touch points that allow networked emerging capabilities to achieve decentralized, coordinated action and effects through the human domain, improving the agility and effectiveness of the Joint Force.

15. SUBJECT TERMS
Asymmetric Capabilities, Cyberspace, Special Operations Forces, Self-Synchronizing Networks

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	33	

USAWC STRATEGY RESEARCH PROJECT

Touch Points in Emerging Capabilities: Cyber, Space, and Special Operations

by

Colonel Mark E. Orwat
United States Army

Professor William O. Waddell
Center for Strategic Leadership and Development
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	Touch Points in Emerging Capabilities: Cyber, Space, and Special Operations
Report Date:	15 April 2014
Page Count:	33
Word Count:	6,727
Key Terms:	Asymmetric Capabilities, Cyberspace, Special Operations Forces, Self-Synchronizing Networks
Classification:	Unclassified

A key effort in developing Joint Force 2020 is to “pioneer new ways to combine and employ emergent capabilities such as cyber, Special Forces, and ISR” and “examine organizational and other force development changes to better leverage game-changing capabilities.” Individually, the emerging capabilities are maturing in capability, capacity, and integration into military operations. However, collectively, the emerging capabilities are not advancing with respect to each other. This strategic research paper draws from my personal experience working in the three emergent areas and includes a comprehensive review of visionary concepts such as Joint Force 2020, SOCOM 2020, and LandCyber 2018-2030. Major touch points exist between emerging capabilities in terms of interoperable technology, organizational integration, and combined effects that will enable self-synchronization among networked cyber, space, and Special Operations Forces in support of the Joint Force. This research establishes touch points that allow networked emerging capabilities to achieve decentralized, coordinated action and effects through the human domain, improving the agility and effectiveness of the Joint Force.

Touch Points in Emerging Capabilities: Cyber, Space, and Special Operations

> The Joint Force will also be used differently. Specialized capabilities, once on the margins, will move to the forefront. Networked special operations, cyber, and Intelligence, Surveillance, and Reconnaissance (ISR) will become increasingly central.
>
> —General Martin Dempsey[1]

By issuing his "18th Chairman's Strategic Direction to the Joint Force," the Chairman, Joint Chiefs of Staff (CJCS), articulated this vision for the Joint Force 2020. A key effort in developing Joint Force 2020 is to "pioneer new ways to combine and employ emergent capabilities such as cyber, Special Forces, and ISR" and to "examine organizational and other force development changes to better leverage game-changing capabilities."[2] A subset of space-based assets allows for the persistent collection of information through surveillance and reconnaissance activities and is considered a challenging component of the ISR infrastructure.[3] Individually, the emerging capabilities of cyber, space, and Special Operations are maturing in capability, capacity, and integration into a conventional Joint Force that is centered on Land, Sea, and Air components. However, collectively, the emerging capabilities are not advancing with respect to each other. Major touch points exist between emerging capabilities in terms of interoperable technology, organizational integration, and combined effects that will enable self-synchronization among networked cyber, space, and Special Operations Forces (SOF) in support of the Joint Force.

The touch points facilitate self-synchronization, a term first used in conjunction with Network Centric Warfare theory and later extended to the SOF global network approach. Initially, self-synchronization first described a mode of interaction between entities that served as "the ultimate in achieving increased tempo and responsiveness"

in Network Centric Warfare.[4] The key elements of self-synchronization were “two or more robustly networked entities, shared awareness, a rule set, and a value-adding interaction” that enable decentralized action.[5] The SOF approach allows the networked entities to share information, to develop a shared situational awareness, and “to achieve a degree of self-synchronization” defined as “an understanding of what the other person in the node brings and how to tap into it.”[6] Self-synchronization between the emerging capabilities will enable decentralized, coordinated action in line with the philosophy of mission command and result in a more agile, effective Joint Force.[7]

To most effectively communicate the touch points, this paper begins with an overview of the United States’ (US) interests and national strategic guidance that has led to the vision of a Joint Force that harnesses emerging capabilities. Next, the paper outlines an existing attempt to interrelate the capabilities as related to deterrence theory. The paper then details the touch points between cyber, space, and SOF. Finally, the paper highlights the recommendations, risks, and conclusions that derive from the touch points.

United States Interests and National Strategic Guidance

The United States’ ability to achieve its national interests in furthering economic prosperity and maintaining a stable international order depends on the unimpeded use of space and cyberspace as well as the existence of an agile, cost effective military to “ensure our nation remains immune from coercion.”[8,9] To shape the military force, the President of the United States (POTUS), the Secretary of Defense (SECDEF), and the CJCS have issued complementary national strategic guidance calling for a future military with increased reliance on cyber, space, and SOF.

The President clearly communicated his strategic vision to the senior military leadership prior to the 2012 Defense Strategic Review.

> As we look beyond the wars in Iraq and Afghanistan -- and the end of long-term nation-building with large military footprints -- we'll be able to ensure our security with smaller conventional ground forces. We'll continue to get rid of outdated Cold War-era systems so that we can invest in the capabilities that we need for the future, including intelligence, surveillance and reconnaissance, counterterrorism, countering weapons of mass destruction and the ability to operate in environments where adversaries try to deny us access. [10]

Through this speech and subsequent strategic guidance, the President has expressed his vision for the military's role in protecting national security. While directing increased investments in future capabilities, he has charged the Department of Defense (DoD) with developing "innovative, low-cost, and small-footprint approaches to achieve our security objectives."[11] These constraints on future military operations affect DoD's military capability development and employment in support of national security objectives.

The Department of Defense recognized the impact that emerging capabilities such as space, cyber, and SOF have had on recent military operations and has embraced the President's vision for the future military. The SECDEF, in a November 2013 keynote address before the Center for Strategic and International Studies' Global Security Forum, stated that "the fourth (budget and strategic planning) priority will be protecting investments in emerging military capabilities -- especially space, cyber, special operations forces, and intelligence, surveillance and reconnaissance." [12] The SECDEF further stated that the emerging capabilities and other non-traditional decisive technologies will ensure global freedom of access for the Joint Force. The senior military advisor to POTUS and the SECDEF is shaping the future Joint Force around

the related strategic guidance. In his second term guidance, the CJCS reemphasizes his Joint Force 2020 vision to include the need to “develop, test, and refine concepts for the future fight” that includes an integrated SOF, ISR and cyber network.[13]

Finally, the 2014 Quadrennial Defense Review (QDR) reflects the above strategic guidance by rebalancing the Joint Force so that it “remains modern, capable, and ready” by protecting “key capability areas.” The areas include cyber, space, ISR, and Counter Terror and Special Operations.[14] The QDR provides the means to allow DoD to mature the emerging capabilities both individually and collectively. To date, the only effort attempting to combine the three emerging capabilities is the creation of a theory in the area of deterrence.

Emerging Capabilities as a Deterrent

The DoD community has only just begun to “pioneer new ways to combine and employ emergent capabilities such as cyber, Special Forces, and ISR.”[15] Currently, the individual communities responsible for the emerging capabilities remain focused on maturing the critical technologies, building capacity to support global operations, and integrating the resources into the Joint Force. A notable exception to the separate efforts is the thought piece offered by a former NATO Supreme Allied Commander Europe.

The thought piece suggests combining emerging capabilities into a “New Triad” for the 21st Century. The “’New Triad’ consists of special operations forces, unmanned vehicles, and cybercapabilities.”[16] Like the cold war strategic triad based on nuclear weapons, the “New Triad” can serve as a deterrent in future US security operations. Yet, the “New Triad” will be “far less abstract and hidden-away than the Cold War strategic triad and much more frequently employed – often in kinetic ways.”[17] Although

the “New Triad” deterrent model combines emerging capabilities, the capabilities may be leveraged individually as would the delivery systems for the current strategic nuclear deterrent triad. The commentary further suggests that the DoD community “create synergies between the branches of this New Triad” and think about how the various research and development efforts may be “fused effectively.”[18]

“Touch Points of Emerging Capabilities: Cyber, Space, and Special Operations” does not further this deterrence triad idea, but focuses on ways to combine the emerging capabilities of cyber, space, and SOF. Currently, these three emerging capabilities are rapidly maturing in isolation with limited integration across the capabilities.

Emerging Capability Touch Points

The following touch points illustrate ways in which cyber, space, and SOF capabilities intersect from the standpoint of interoperable technology, organizational integration, and combined effects. Specific touch points include the collapse of the space and cyber domains, operating through the human domain, countering Anti-Access / Aerial Denial, Geographical Combatant Commander theater integration, global mission integration, establishing a holistic common operating picture, and building an infrastructure for future mass deployment of robotics. Once fully realized, these touch points will enable the emerging capabilities to self-synchronize and provide increased tempo and responsiveness to the Joint Force.

The Collapse of the Space and Cyber Domains

The current cyber domain consists of a physical and virtual network of communications and sensory equipment. The domain includes terrestrial, maritime, and aerial networks combined together in a global network. The space domain, with its

autonomous collection of networks and sensors, is yet to be fully integrated into this cyber domain. Technology is driving a merger of the space and cyber domains that will enable space-based platforms to become standard nodes on the network.

The research community is introducing packet-based technologies into space platforms that allow a seamless interface with ground-based networks.[19] Additionally, commercial entities are developing communications routers for space that use the Internet Protocol (IP), also a packet-based network implementation.[20] With these technical advancements, satellites will be able to send and receive command and control, telemetry, and return data messages without having to convert between different formats. Future network communications will route to and from the terrestrial infrastructure and the space communications architecture in a seamless fashion.

To take full advantage of this advancement, satellite platforms related to communications; precision, navigation and timing (PNT); intelligence; weather; and anti-satellite capabilities could be considered nodes and sensors in a global cyber network. The other space missions such as space exploration and manned flight do not necessarily have to be incorporated into the cyber domain outside of utilizing the communications links. These research and development efforts can remain separate from the cyber domain and can constitute the totality of the activity in the reduced space domain.

Creating a merged cyber and space network, although exposing space-based assets to increased cyber risk, will greatly enhance the robustness of the global network. If partially merged with cyberspace, the space platforms would become targets of cyber activity and would need enhanced network security features. Space systems

will add to the vast array of unmanned ISR and communications capabilities available in the cyber domain by offering the ability to operate in a persistent fashion over denied areas of the world.[21] With a merged cyber and space domain, the cyber and SOF entities can better leverage the network to influence the human domain.

Operating Through the Human Domain

Cyber, space, and SOF operate within and significantly influence the human domain. Although a controversial term in military art, the human domain "encompasses the totality of the physical, cultural, and social environments that influence human behavior."[22] Capabilities in the three emergent areas are typically applied independently in attempts to influence the thoughts and actions of different groups of people. Synchronizing a merged cyber and space network with the existing global SOF network could bring unity of effort to military activity within the human domain and could ensure that military operations are planned and executed with a deeper understanding of the "reacting human populations and the virtual networks those humans use to communicate."[23]

People are highly dependent on cyberspace and satellites for many aspects of modern life. The economic prosperity of the nation depends on the ability of the communications, transportation, energy, banking, and finance industries to function in the cyberspace and space domains.[24] The populace relies on these same industries to subsist, conduct business, and interact socially. The military counts on capabilities in cyberspace and space to accomplish tasks across the joint warfighting functions of command and control, intelligence, fires, movement and maneuver, protection, and sustainment.[25] The most recent joint warfighting concepts: Air Sea Battle, Landpower, LandCyber, and the Joint Operational Access Concept (JOAC) all highlight the

dependency of successful military operations on effective action in the cyberspace and space domains.[26,27,28,29] The biggest challenge to military operations in a merged cyber and space domain is the lack of cyber Intelligence, Surveillance, and Reconnaissance (ISR).[30]

The Joint Force "lacks adequate cyberspace-based surveillance and reconnaissance systems" resulting in an inability to understand the effects of cyberspace operations on the will of the people.[31] The effects of basic information operations delivery, such as the change of content on an adversary's web page, is not fully understood, let alone the effects of full scale offensive cyberspace operations.[32] "Knowing what motivates the people, what incentivizes the people, what mobilizes the people, what frightens them, and what will undermine their will" gives insight into the true effects of physical and virtual global engagement.[33] SOF has a long history of effectively understanding the environment and the populace and can help meet the cyber ISR challenge by envisioning and assessing the effect of a cyberspace or space activity on the will of the people.

As the most widely known small-footprint military capability, SOF has been employed worldwide since the three-man Jedburgh teams provided leadership to French Resistance units in World War II.[34] Currently, SOF is serving in 70 countries, with most missions "supporting U.S. embassies, training foreign forces or strengthening bonds with allied militaries."[35] Besides this continuous widespread activity related to steady state operations, the United States Special Operations Command (USSOCOM) is responsible for the global counterterrorism mission. SOF elements maintain regional, cultural, and linguistic familiarization that aid in a fuller understanding of a population.

SOF is considered the “connective tissue between the population and military forces.”[36] As such, a future merged cyberspace and space mission force can leverage SOF expertise and infrastructure to more effectively employ capabilities.

SOF has built an extensive global infrastructure that the cyberspace and space mission forces could leverage. An emerging initiative in the Special Operations community is the Global SOF Network. The concept is to “establish a formal framework in which US special operations forces (SOF), interagency partners and foreign allies join an alliance that promotes the sharing of intelligence, partner engagement, training and, if necessary, direct action.”[37] SOF has a tight integration with interagency partners established over the course of the prosecution of the global war on terror. Besides a network of people, SOF maintains its own robust communications network, funded and managed internally, which gives SOF the ability to move high-bandwidth ISR feed around the operational area and back to a comprehensive common operating picture (COP) at USSOCOM headquarters.[38] Rather than building a parallel capability, the cyberspace and space personnel could work through the SOF infrastructure.

The emerging capabilities can work closer together at the tactical edge, closest to the populace, to deliver synchronized effects. SOF can take advantage of initiatives in the space domain such as Operational Responsive Space, smaller tactical satellite systems such as cubesats, and lighter boosters for expedient launches to gain more responsive space capability without having to compete for National Space Systems and overhead collection assets.[39] Additionally, SOF and cyber forces can use tactical devices to access preprocessed information from overhead collection platforms. SOF continues to rely on satellite-based expeditionary communications systems when

deployed around the world. The possibility of space-enabled cyber effects in non-permissive areas of the world has a lot of potential for SOF and cyber forces. By developing an independent cyberspace access capability, cyber forces can move cyber activity and coordination away from national access centers towards the tactical edge and the people upon which the cyber effect is focused.[40] Finally, SOF and cyber forces can join to conduct close-in cyberspace injects to gain more localized effects. Injects may include radio frequency actions, thumb drive injects, cell tower jamming, fiber cuts, and electronic warfare.

Cyber, space, and SOF impact the human domain. By working together at the tactical edge within the physical and virtual networks of the populace, combined effects may be better assessed to include the reaction of the people. Shared understanding, common situational awareness, and self-synchronization add tempo and responsiveness to the Joint Force.

Countering Anti-Access / Area Denial (Supporting the Joint Operational Access Concept)

The strengths of an integrated cyber, space, and SOF capability, while enabling more effective operations in the human domain, are also central to countering Anti-access / Area Denial (A2/AD). Adversarial nations are focusing on weakening the ability of the US military to project power around the world into areas deemed critical to the national interest.[41] US power projection capabilities include aircraft carriers, troop ships, and large transport aircraft along with the cyberspace and space-based command and control aspects that enable them. Threat weapon development and procurement is focused on asymmetric capabilities such as over the horizon radar, ballistic missiles, anti-satellite weapons, submarines, and cyber warfare tools.[42]

To counter the asymmetric A2/AD threat and enable greater freedom of movement and maneuver to project the Joint Force into a non-permissive area, the US must rely on comparable asymmetric capabilities. The SECDEF stated “as our potential adversaries invest in more sophisticated capabilities and seek to frustrate our military's traditional advantages, including our freedom of action and access … around the world, it will be important to maintain our decisive technological edge.”[43] The JOAC describes how the Joint Force will counter A2/AD actions by attempting to integrate capabilities across the various warfighting domains, including cyber and space, and achieving “cross-domain synergy.”[44] The innovative and small-footprint approaches inherent in cyber, space, and SOF naturally lead to an increased ability for the joint force to operate within areas of denied access. A cohesive cyber, space, and SOF action can have a localized, population-sensitive effect on the adversary’s A2/AD system with the added benefit of a robust return feedback loop for enhanced situational awareness. Achieving cross-domain synergy to counter A2/AD threats around the world requires the integration of asymmetric capabilities within the Geographic Combatant Command (GCC).

Geographical Combatant Commander Theater Integration (Unity of Effort)

The DoD has innovative, small footprint capabilities in cyber, space, and SOF that can operate through the human domain and counter the anticipated A2/AD threat if properly synchronized within the GCC. The major challenge facing the GCC is the integration of the emerging capabilities into a deployable force structure across the operational phases of the campaign.

The GCCs have an integrated warfighting capability with which to effectively operate in the geographically defined domains of land, maritime, and air. The

Goldwater-Nichols DOD Reorganization Act of 1986 established unity of joint command and forced the individual services to collaborate in terms of integrated planning, shared procurement, and joint training.[45] As a direct result of the implementation of this Act, the GCCs are assigned and allocated ground, naval, and air forces that are accustomed to operating jointly across the full range of military operations. The emerging domains are not as tightly integrated. The GCCs tend to view cyberspace, space, and SOF capabilities as platforms from which to project and to command and control conventional, large footprint ground, sea, and air capabilities. Instead, the GCCs need to find ways to conduct warfighting operations in the cyber and space domains to achieve cyber, space and SOF effects that complement the traditional domains.

Further complicating the integration of the emerging capabilities into GCC planning and execution is a lack of clear authorities. Currently, the GCC staffs have personnel that can facilitate the integration of the emerging capabilities, but the corresponding authorities are not clearly established and the joint doctrine facilitating the integration has yet to be developed. Within the GCC, SOF is represented by the Theater Special Operations Command (TSOC), the cyber forces by the Joint Cyberspace Center (JCC), and the space assets by a mission dependent collection of space operators potentially as large as a Joint Space Element.[46] The full integration of each planning and execution group is limited by complex command relationships that result in unclear authorities. For example, the TSOC reports directly to USSOCOM and the JCC reports to the United States Cyber Command (USCYBERCOM). The GCC does have operational control of all of the elements. To complicate integration further, since cyberspace effects are not well understood, the GCC must coordinate the use of

cyberspace capabilities with USCYBERCOM, which in turn deploys the cyber capabilities for the Joint Force.[47]

The Cyber Mission Force has elements that are responsible for integrating cyber planning and coordinating cyber effects. However, the ability to fully integrate with the GCC is limited by physical separation. Currently, the elements have to be collocated with national access capabilities, away from the GCC. The JCC provides a small liaison group, but the cyber operators that actually plan and execute the real cyber effects are not. Additionally, the co-use of the access platforms forces the cyber elements to restrict their activities to national priorities at the expense of the GCC priorities. With the development and procurement of an independent access capability, cyber operators could be closer to the GCC planning staffs and more responsive to GCC priorities, thus increasing unity of effort at the GCC.

For total unity of effort at the GCC, a merged cyber and space domain with more robust, independent capabilities can plan and execute from the Joint Cyber Control Center (JCCC).[48] When conducting operations through the traditional warfighting domains as well as in the cyber and space domains, GCC planners may find a higher level of synchronization through a tighter coupling of the TSOC and the JCCC. Forces operating through the human domain using the SOF established communications network will forward valuable situational awareness to the GCC common operating picture (COP).

In terms of doctrine, separate joint publications exist for Special Operations, Cyberspace Operations, Information Operations, Electronic Warfare, Space Operations, and Counter Terrorism. A joint publication does not exist for the holistic integration of

the emerging capabilities across the domains.[49] As a result, the GCC's application of the emerging concepts towards operational military objectives often lacks an effective level of synchronization.

With an increase in synchronization across the emerging capabilities, the GCC may better employ cyber, space, and SOF capabilities during steady state operations and campaign Phase 0 shaping operations such as multinational exercises, rotational presence, and advisory capabilities and avoid internal problems leading to escalation. US persistent forward presence and use of cyber and space sensors could provide intelligence back to the GCC for phase escalation decisions and staff problem and environment re-framing. With global military activity, the potential for interagency discord and de-synchronization is high. SOF has the network and personnel to effectively work within the interagency.

A tighter integration of the emerging capabilities at the operational level increases the unity of effort and improves cross-domain and interagency synchronization during GCC planning and execution. The result is a greater impact during steady state and early phases of the campaign, more effective ability to overcome A2/AD and maintain freedom of action, and an increased joint warfighting capability to the GCC. Self-synchronization at the GCC is also achievable at the national level.

Global Mission Integration (Unity of Effort)

Integrating the emerging capabilities is also important to the overall unity of effort at the national level. The challenges and opportunities in integrating cyber, space, and SOF at the national level derive from many of the touch points at the operational level and on the tactical edge.

SOF has built extensive organizational experience and a robust infrastructure in the prosecution of its global counterterrorism mission through the human domain.[50] Cyber and space missions also tend to be global in nature. SOF emphasizes a global network of SOF, a worldwide communications network with sufficient capacity to provide global situational awareness back to USSOCOM headquarters. As discussed earlier, activity in the cyber and space domains must integrate with SOF in the application and understanding of the totality of the effects in the human domain at the national level. A merged cyber and space capability could leverage the SOF global communications network to deliver its effects. A national common operating picture (COP), using the current robust SOF COP as a base, could be augmented with cyber and space information and activities in order to present a more holistic picture of global effects of the emerging capabilities. Including the portions of the Cyber Mission Force that are focused on protecting our nation's critical infrastructure into the COP will yield an even more complete picture. The same exact COP may be fed to various commands (e.g., GCCs, USCYBERCOM, USSOCOM) and national decision makers so as to enable shared situational understanding and synchronized effects.

SOF has purposefully built a strong presence within the National Capital Region (NCR) in order to look after SOF equities. The physical proximity to national level decision makers in both the government and the interagency allows for tighter synchronization and mission effectiveness.[51] The result is a better understanding of the national importance and the global effects of the SOF mission. SOF remains funded at a high level and benefits from its own Major Funding Program (MFP) line, MFP-11.[52] MFP-11 is designed to fund acquisitions that are SOF-specific for use in the global war

on terror. The merged cyber and space activity should leverage the SOF political infrastructure in the NCR in order to assist in its strategic messaging with national decision makers and the protection of investments into the emerging capabilities. The importance of a shared global situational awareness cannot be understated and is directly enabled by an integrated COP.

Establishing a Holistic Common Operating Picture

When using the emerging capabilities in a decentralized fashion in the human domain, an integrated COP is essential to achieving synchronized effects. Localized operations, in line with the mission command approach of Joint Force 2020, require a shared understanding of the action and the effects on the population.[53] A COP may yield different views depending upon the level of command, from a national perspective down to the tactical edge. The COP could inject interagency data to ensure unity of effort across the organizations. Cyber, space, and SOF tend to have local effects, and looking at the three activities holistically will achieve critical self-synchronization. Although the USSOCOM COP is a very robust system, the technology behind the COP has to be improved in order for the rest of the emerging capabilities to be able to leverage the infrastructure.

A COP that includes feed from cyberspace, space, SOF, and interagency activities has to be very sophisticated given the infusion of technology that delivers ubiquitous sensor data, high volumes of information and intelligence, and extensive communications. A single, commander-focused COP platform must be able to cross multiple security classification domains in order to allow for information sharing. Additionally, the COP platforms have to be able to ingest the entirety of the intelligence collections and communications systems present on a global scale. The Joint Vision

2020 unequivocally states the proliferation of information technology will make "information superiority a key enabler of the transformation of the operational capability of the joint force and the evolution of joint command and control."[54] A single COP will ensure that the commanders have as complete a picture as possible prior to making the difficult decisions. The final touch point in the emerging capabilities is the deployment of robotic capabilities.

Building an Infrastructure for the Future Mass Deployment of Robotics

The final touch point where the integration of the emerging capabilities has considerable promise is the deployment and control of unmanned military forces. This touch point is futuristic with a heavy reliance on developing technology. Currently, robotic technologies are pervasive in the joint operational area including unmanned aerial vehicles and submersibles, unmanned light ground combat vehicles, cave explorers, and smaller satellites. A significant challenge with military robots is "coordinating and controlling all the different unmanned systems in the incredibly complex environment of battle."[55] The Joint Force could heavily leverage all three of the emerging capabilities in the development of the infrastructure to allow the successful deployment of mass robotics.

Small footprint SOF teams with cyberspace and space expertise could provide command and control and report back accurate assessments of the effects of military operations to the COP. The polarizing nature of artificial intelligence and robotics makes it important to understand not only "the effects on the field of battle, but also among the broader populace."[56] SOF can assist in providing human context and populace reaction to deployed robots. SOF is comfortable operating in hostile areas while leveraging advanced technology and can bring that same expertise to the deployment of

unmanned units. Mass deployments of robots will require communications on the move and highly networked, coordinated nodes. Cyberspace capabilities will be essential to protect and command and control the robots. Space will enable satellite controlled autonomous systems over non-permissive areas with a persistent presence.

Although years away in development, the successful mass deployment of robotics will necessitate tightly integrated cyber, space, and SOF capabilities. A self-synchronized network of emerging capabilities will ensure that unmanned capabilities are fully responsive to the Joint Force.

Recommendations

Several recommendations result from the identified touch points that will enable future self-synchronization among networked cyber, space, and SOF.

Once the technology is ready, DoD must merge the cyber domain with the unmanned portion of the space domain in order to provide an integrated infrastructure and coordinated effects. When considering space platforms as nodes on the network, DoD must ensure that the assets are connected through a secure network in order to prevent successful cyber attacks on the critical US satellite constellations.

DoD must integrate the merged cyber and space capabilities with SOF in order to provide unity of effort at the tactical edge. The small, agile, technical teams can conduct decentralized activity against asymmetric adversaries. The integrated emergent capability can better operate through the human domain and more effectively apply cyber, space, and SOF effects on the populous. Cyber ISR and situational awareness of the decentralized operations and coordinated effects will improve dramatically.

The merged cyber and space capability must be allowed to leverage the robust SOF worldwide communications network. Despite the difference in classification levels and compartments, using the same network will have a self-synchronizing effect.

The cyber, space, and SOF planning and execution entities within the GCC must have a tighter integration when planning steady state and early phases of a campaign. The TSOC and JCCC must synchronize activity within the GCC and ensure that the combined effects are clear. DoD must publish joint doctrine related to the integration of cyber, space, and SOF activities.

The cyberspace and space communities must leverage the existing SOF national level infrastructure. The SOF presence within the NCR will enable the communities to better communicate the portfolio of emerging capabilities and the resulting population effects to national decision makers. A merged funding line such as Major Force Program 11 can assist in meeting funding shortfalls in the employment of emerging capabilities. The SOF infrastructure that provides a worldwide COP must be used to ingest cyberspace and space events and effects in order to enhance the shared understanding at all levels of joint operations.

Lastly, the science and technology community must continue its pursuit of both cyberspace access platforms and robotics technology as future sources of Joint Force capability. The research and development should consider the small-footprint, secure command and control of mass deployments of unmanned capability in a non-permissive environment.

When implemented in total, the recommendations will stitch together interoperable technologies, organizational integration, and combined effects that will

enable self-synchronization among networked cyber, space, and SOF. Several risks impede the possible realization of these recommendations.

Risks

Several challenges impede the complete synchronization of the cyber, space, and SOF capabilities.

The cyber domain is rapidly maturing in terms of capabilities and effects. The continual change in this domain could serve to desynchronize integration efforts. Authorities and permissions to execute cyberspace operations are still at the National Command Authority level per Presidential Policy Directive 20, which inhibits decentralized actions.[57]

The cyber, space, and SOF communities have different cultures that may hinder integration. For example, SOF has a culture of decentralized combat operations with a focus in the human domain, cyber forces focus on computer networks, and the satellite community is tightly connected to the US Air Force.

All three emerging capabilities do not have the capacity to accommodate the worldwide mission. There are not enough of the specialized elements in existence to fully integrate at the national level, operational level, and tactical edge.

Information classification levels and compartments exist to prevent the loss of intelligence sources within all three emerging communities. The same security measures will hinder synchronized operations.

In the current fiscally informed environment, national decision makers may see the additional infrastructure required to integrate the emerging capabilities as overly expensive. The Global SOF Network and the cyberspace access capability could be

seen as a redundant even though they are both critical to integrating Joint Force effects in the human domain.

An enhanced common operating picture that incorporates cyber, space and SOF data at all levels of military operations may increase the tendency for high-level oversight. The result will be more centralized control of local populous effects, which is counter to the current Joint Force philosophy of mission command.

Lastly, the public debate over robotics and unmanned military operations in terms of ethics and true effects on the will of the people may slow the deployment of mass robotic formations during Joint Force operations.

Conclusions

> US military power today is unsurpassed on the land and sea and in the air, space, and cyberspace. The individual Services have evolved capabilities and competencies to maximize their effectiveness in their respective domains. Even more important, the ability to integrate these diverse capabilities into a joint whole is greater than the sum of the Service parts is an unassailable American strategic advantage.[58]

National level strategic guidance specifically directs the integration of emerging capabilities in order to “better leverage game-changing capabilities.”[59] Major touch points exist between emerging capabilities in terms of interoperable technology, organizational integration, and combined effects that will enable self-synchronization among networked cyber, space, and Special Operations Forces in support of the Joint Force. Specific touch points include the collapse of the space and cyber domains, operating through the human domain, countering Anti-Access / Aerial Denial, Geographical Combatant Commander theater integration, global mission integration, establishing a holistic common operating picture, and building an infrastructure for future mass deployment of robotics.

Fully developing the specified touch points will enable the network of emerging capabilities to self-synchronize, to provide enhanced effects through the human domain, and to offer increased tempo and responsiveness to the Joint Force. Even in the current fiscally informed environment, DoD must build a self-synchronized network of emerging capabilities to sustain the "unassailable American strategic advantage" and keep the United States free from coercion.[60]

Endnotes

[1] U.S. Joint Chiefs of Staff, *18th Chairman's Strategic Direction to the Joint Force* (Washington, DC: U.S. Joint Chiefs of Staff, February 6, 2012), 6.

[2] Ibid., 8.

[3] U.S. Joint Chiefs of Staff, *Space Operations*, Joint Publication 3-14 (Washington, DC: U.S. Joint Chiefs of Staff, January 6, 2009), A-1.

[4] David Alberts, John Garstka, and Frederick Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority,* 2nd ed. (Washington, DC: CCRP Publications Series, 1999), 175.

[5] Ibid., 176.

[6] Claudette Roulo, "McRaven: Success in Human Domain Fundamental to Special Ops," June 5, 2013, http://www.defense.gov/news/newsarticle.aspx?id=120219 (accessed March 20, 2014).

[7] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0 (Washington, DC: U.S. Joint Chiefs of Staff, August 11, 2011).

[8] Barack H. Obama, *National Security Strategy* (Washington, DC: The White House, May 2010), 17.

[9] Martin E. Dempsey, "General Dempsey's Letter to the Joint Force," October 1, 2011, http://www.dodlive.mil/index.php/2011/10/general-dempseys-letter-to-the-joint-force/ (accessed March 4, 2014).

[10] White House Office of the Press Secretary, *Remarks by the President on the Defense Strategic Review* (Washington, DC: Office of the Press Secretary, January 2012), 1.

[11] U.S. Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: U.S. Department of Defense, January 2012), 3.

[12] Cheryl Pellerin, "Hagel: Six Priorities Shape Future Defense Institutions," November 5, 2013, http://www.defense.gov/news/newsarticle.aspx?id=121054 (accessed November 20, 2013).

[13] U.S. Joint Chiefs of Staff, *18th Chairman's 2nd Term Strategic Direction to the Joint Force* (Washington, DC: U.S. Joint Chiefs of Staff, January 17, 2014), 6.

[14] Chuck Hagel, *Quadrennial Defense Review 2014* (Washington, DC: U.S. Department of Defense, March 2014), X-XI.

[15] U.S. Joint Chiefs of Staff, *18th Chairman's Strategic Direction to the Joint Force* (Washington, DC: U.S. Joint Chiefs of Staff, February 6, 2012), 6.

[16] James Stavridis, "The New Triad, It's Time to Found a U.S. Cyber Force," *Foreign Policy*, 2013.

[17] Ibid.

[18] Ibid.

[19] Clayton Okino, Andrew Gray, and Joshua Schoolcraft, "Protocol Sensing across Multiple Space Missions," June 2007, http://trs-new.jpl.nasa.gov/dspace/bitstream/2014/39703/1/06-2007.pdf (accessed March 22, 2014).

[20] Enrique G. Cuevas, Hadi A. Esiely-Barrera, H. Warren Kim, and Zhuangbo Tang, "Assessment of the Internet Routing Protocol in Space-Joint Capability Technology Demonstration," *Johns Hopkins APL Technical Digest* 30, no. 2 (2011): 5.

[21] U.S. Joint Chiefs of Staff, *Space Operations*, Joint Publication 3-14 (Washington, DC: U.S. Joint Chiefs of Staff, January 6, 2009).

[22] Claudette Roulo, "McRaven: Success in Human Domain Fundamental to Special Ops," June 5, 2013, http://www.defense.gov/news/newsarticle.aspx?id=120219 (accessed March 20, 2014).

[23] Sydney J. Freedberg, "People, Cyber & Dirt: Army & SOCOM's 'Strategic Landpower'," *Breaking Defense,* October 24, 2013, http://breakingdefense.com/2013/10/people-cyber-dirt-army-socoms-strategic-landpower/ (accessed March 10, 2014).

[24] U.S. Joint Chiefs of Staff, *Space Operations*, Joint Publication 3-14, A-1.

[25] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, III-1.

[26] U.S. Department of Defense, *Air-Sea Battle: Service Collaboration to Address Anti-Access and Aerial Denial Challenges* (Washington, DC: U.S. Department of Defense, May 2013).

[27] Raymond T. Odierno, James F. Amos, and William H. McRaven, "Strategic Landpower, Winning the Clash of Wills," February 5, 2013,

http://www.tradoc.army.mil/FrontPageContent/Docs/Strategic%20Landpower%20White%20Paper.pdf (accessed January 15, 2014).

[28] U.S. Department of the Army, *United States Army LandCyber White Paper: 2018-2030* (Washington, DC: U.S. Department of the Army, February 05, 2013).

[29] U.S. Department of Defense, *Joint Operational Access Concept (JOAC), Version 1.0* (Washington, DC: U.S. Department of Defense, January 17, 2012).

[30] Brett T. Williams, "Cyberspace Operations," lecture, U.S. Army War College, Carlisle Barracks, PA, March 04, 2014, cited with permission of Mr. Williams.

[31] U.S. Department of the Army, *United States Army LandCyber White Paper: 2018-2030*, 22.

[32] Williams, "Cyberspace Operations."

[33] Freedberg, "People, Cyber & Dirt: Army & SOCOM's 'Strategic Landpower'."

[34] Colin Beavan, *Operation Jedburgh: D-Day and America's First Shadow War* (New York: Penguin Group, 2006), 3.

[35] Stew Magnuson, "Special Operations Missions to Require New Doctrine," *National Defense Magazine,* May 2013, http://www.nationaldefensemagazine.org/archive/2013/May/Pages/SpecialOperationsMissionstoRequireNewDoctrine.aspx (accessed January 6, 2014).

[36] William H. McRaven, "SOF 2020," lecture, U.S. Army War College, Carlisle Barracks, PA, February 20, 2014, cited with permission of Mr. McRaven.

[37] U.S. Special Operations Command, *SOCOM 2020* (Washington, DC: U.S. Special Operations Command, January 6, 2009), 5.

[38] McRaven, "SOF 2020."

[39] Sheila Rupp, "Operationally Responsive Space," May 22, 2007, http://www.kirtland.af.mil/news/story.asp?id=123054292 (accessed January 15, 2014).

[40] Williams, "Cyberspace Operations."

[41] U.S. Department of Defense, *Joint Operational Access Concept (JOAC), Version 1.0*, ii.

[42] Ibid., 9-10.

[43] Pellerin, "Hagel: Six Priorities Shape Future Defense Institutions."

[44] U.S. Department of Defense, *Joint Operational Access Concept (JOAC), Version 1.0*, ii.

[45] *Goldwater-Nichols Department of Defense Reorganization Act of 1986*, House of Representatives Bill 3622, 99th Cong. (October 24, 1985).

[46] U.S. Joint Chiefs of Staff, *Space Operations*, Joint Publication 3-14, III-3.

[47] Zachary Fryer-Biggs, "U.S. Military Goes on Cyber Offensive," March 24, 2012, http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive (accessed January 15, 2014).

[48] Williams, "Cyberspace Operations."

[49] U.S. Joint Chiefs of Staff, *Joint Electronic Library* (Washington, DC: U.S. Joint Chiefs of Staff, 2014).

[50] U.S. Special Operations Command, *SOCOM 2020,* 1-7.

[51] Ibid., 5.

[52] U.S. Department of Defense, *SOF Resource Overview* (Washington, DC: U.S. Department of Defense), 39, http://www.dod.mil/pubs/sof/resource.pdf (accessed March 10, 2014).

[53] McRaven, "SOF 2020."

[54] U.S. Department of Defense, *Joint Vision 2020 (*Washington, DC: U.S. Joint Chiefs of Staff, June 2000), 3.

[55] Peter W. Singer, *Wired for War, the Robotics Revolution and Conflict in the Twenty-first Century* (New York: Penguin Press, 2009), 202.

[56] Ibid., 309.

[57] Electronic Privacy Information Center, "Presidential Directives and Cybersecurity," http://epic.org/privacy/cybersecurity/presidential-directives/cybersecurity.html (accessed March 18, 2014).

[58] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, III-1.

[59] U.S. Joint Chiefs of Staff, *18th Chairman's Strategic Direction to the Joint Force* (Washington, DC: U.S. Joint Chiefs of Staff, February 6, 2012), 6.

[60] U.S. Joint Chiefs of Staff, *Joint Operations*, Joint Publication 3-0, III-1.