Joint Operating Environment

JOE 2035

The Joint Force in a Contested and Disordered World

14 July 2016

Foreword

Although conflict, violence, and war endure, the methods through which political goals are pursued are always evolving. How this change in the character of conflict will play out and what the Joint Force must do to prepare to meet the demands of tomorrow requires our collective attention.

Looking ahead, competitive behavior between the U.S. and potential – and actual – adversaries will be overt and violent. But just as often, our interaction with competitors will include attempts to deter and deny us our strategic objectives or be marked by ambiguous, but still coercive pursuit of political goals backed by the threat or potential of applied military power. Over the next two decades, both overt and ambiguous competitive interactions between dissimilar military forces will be a normal and recurrent condition for the Joint Force.

Looking into this future is challenging. However, the difficulty in looking ahead does not excuse the military professional from considering the demands of future war. As the ultimate guarantor of the safety and security of the United States, the Joint Force must simultaneously adapt and evolve while neither discounting nor wishing away the future reality of strife, conflict, and war.

To think about the future usefully, we must describe change in a rigorous and credible way. Concurrently, we must creatively account for the unexpected by stepping outside the assumptions and certainties that anchor us to today. The Joint Force will best contribute to a peaceful and stable world by developing capabilities and operational approaches attuned to the evolving character of conflict.

Together, we will use this document – *Joint Operating Environment 2035* – to support and accelerate our future strategy and force planning activities across the Joint Force. It is a primary source of the problem sets addressed through the forthcoming *Capstone Concept for Joint Operations* and related force development activities. The ideas here should encourage a dialogue about what the Joint Force should ***do*** and ***be*** to protect the United States, its allies, its partners, and its interests around the world in 2035.

KEVIN D. SCOTT
Vice Admiral, U.S. Navy
Director for Joint Force Development

Executive Summary

The *Joint Operating Environment 2035* (*JOE 2035*) is designed to encourage the purposeful preparation of the Joint Force to effectively protect the United States, its interests, and its allies in 2035. For the Joint Force, thinking through the most important conditions in a changing world can mean the difference between victory and defeat, success and failure, and the needless expenditure of human lives and national treasure versus the judicious and prudent application of both to defend our vital interests.

This document describes the future security environment and projects the implications of change for the Joint Force so it can anticipate and prepare for potential conflicts. To do this, Section 1 describes the circumstances that are likely to alter the security environment. Next, Section 2 explores how the intersection and interaction of these changes might impact the character of war in the future. Finally, Section 3 provides a framework to think about the full range of Joint Force missions and how they may evolve over time.

JOE 2035 illustrates several ideas about how changes to conflict and war might impact the capabilities and operational approaches required by the future Joint Force. These observations include:

The future security environment will be defined by twin overarching challenges. A range of competitors will confront the United States and its global partners and interests. *Contested norms* will feature adversaries that credibly challenge the rules and agreements that define the international order. *Persistent disorder* will involve certain adversaries exploiting the inability of societies to provide functioning, stable, and legitimate governance. Confrontations involving contested norms and persistent disorder are likely to be violent, but also include a degree of competition with a military dimension short of traditional armed conflict.

These connected challenges are shaped by a wide range of trends and conditions. The future *World Order* will see a number of states with the political will, economic capacity, and military capabilities to compel change at the expense of others. In *Human Geography*, a range of social, economic, environmental, and political pressures will push states past the breaking point, spilling over borders, and creating wide-ranging international problems. The future of *Science, Technology, and Engineering* will see others reaching for technological parity as well as designing innovative mixes of high and low technology that may allow adversaries to more effectively challenge U.S. interests.

The intersection of trends and conditions reveals the changing character of war. The future of conflict cannot be understood in terms of individual trends. Issues and problems intersect, reinforce, and compound across many diverse areas. Sometimes relationships are clear, but more often they interact in unanticipated and surprising ways. Thinking through combinations of trends and conditions over many disciplines allows us to better anticipate changes in the character of conflict and illuminate why the Joint Force may be called upon to address threats to U.S. national interests.

Warfare in 2035 will be defined by six contexts of future conflict. In 2035, the Joint Force will confront *Violent Ideological Competition* focused on the subversion or overthrow of established governments. *Threatened U.S. Territory and Sovereignty* will become increasingly prevalent as enemies attempt to coerce the United States and its citizens. *Antagonistic Geopolitical Balancing* by capable adversaries will challenge the United States over the long term and place difficult demands on the Joint Force over wide areas of the globe. Intimidation, destabilization, and the use of force by state and non-state actors alike will result in *Disrupted Global Commons* and *A Contest for Cyberspace*. Internal political fractures, environmental stressors, or deliberate external interference will lead to *Shattered and Reordered Regions*. Each *Context of Future Conflict* poses a troubling problem space for the Joint Force.

The contexts, when matched with a range of strategic goals, drive an evolving set of missions. The Joint Force must prepare for a wide range of missions designed to address these contexts. This set of *Evolving Joint Force Missions* must at once protect our national interests, deter conflict, punish aggression, or defeat adversaries who act across regions, domains, and functions. These evolving missions will be shaped by a continuum of strategic goals that range from *reactively managing* security challenges to *proactively solving* security threats and imposing U.S. preferred solutions. This span of missions will require a diverse set of capabilities and operational approaches – some of which are not available to the Joint Force today.

The evolving mission set demands new operational approaches and capabilities. Placing too much emphasis on *contested norms* – particularly those high-tech and expensive capabilities to contain or disrupt an expansionist state power – may discount potentially disruptive low-end threats, which have demonstrated a troubling tendency to fester and emerge as surprise or strategic shock for the United States. Conversely, tilting the balance of force development activities towards capabilities designed to counter *persistent disorder* may risk a world in which other great powers or alliances of great powers decisively shift the international order in highly unfavorable ways. Ultimately, the future Joint Force will best contribute to a peaceful and stable world through well-crafted operational approaches attuned to the evolving character of conflict.

***JOE 2035* sets the foundation for the future Joint Force.** The ideas found within *JOE 2035* set the stage for a more detailed conversation about how the Joint Force can achieve success in the future security environment. *JOE 2035* was written to accelerate new ways – or concepts – for the Joint Force to address the likely needs of future strategy and thus, identify a foundation upon which enduring U.S. military advantages can be built. Going forward, *JOE 2035* will orient a wide range of future force development activities and provide an analytic basis for ongoing Joint Concept development efforts, particularly a revision of the *Capstone Concept for Joint Operations* (CCJO).

Table of Contents

Introduction

The Joint Force faces two persistent realities. First, the security environment is always in flux. Change is relentless and occurs in all aspects of human endeavor. Ideas about how human beings should govern one another emerge, spread, and then fade away. Advances in science and technology progress and proliferate. Countries and political groups simultaneously cooperate and compete based on their relative power, capabilities, interests, and ideals. Change in the security environment occurs at an irregular pace, and over time small changes compound to shatter our assumptions. Second, the pursuit of political objectives through organized violence is and will remain a feature of the security environment. Strife, conflict, and war are certain to endure through 2035.

The future confounds even the most rigorous attempts to accurately predict how it will unfold. Because the future is difficult to predict and understand, warfare often resembles "a race between belligerents to correct the consequences of the mistaken beliefs with which they entered combat."[1] *JOE 2035* provides a space for the Joint Force to think through what we must do to prepare for this race. To peer into the future in a reliable – and ultimately useful – way involves considering possibilities. Thinking in terms of possibilities requires us to strike a delicate balance between a credible, thorough description of changing trends coupled with the courage to step outside the certitudes and assumptions of today and imagine the range of potential events that might alter our world.

Purpose

The purpose of *JOE 2035* is to describe the future security environment circa 2035 and project implications of change for the Joint Force so it can anticipate and prepare for potential conflicts. To do this, it poses and then explores three foundational questions. Answers to these questions describe the joint operating environment and suggest ways the Joint Force might prepare for this future. These questions are:

- *What trends and conditions will shape the future security environment?*
- *How will trends and conditions intersect to change the future character of war?*
- *What missions will the Joint Force need to conduct in the future?*

Scope

JOE 2035 does not predict the future or attempt to forecast specific scenarios or events. Instead, it develops a range of possibilities about future conflict by re-imagining the set of factors and circumstances shaping the future security environment. Thinking about the future through the lens of various trends, conditions, contexts, and implications encourages an expanded *understanding* of the scope of the problems facing the Joint Force as well as promising avenues to pursue solutions, and supports a broader *appreciation* of the implications of change that will confront the future Joint Force.

JOE 2035 occupies a unique space in the broader effort to prepare the U.S. military for future war. It does not replace specific planning scenarios, but is a backdrop for a range of joint force development activities across the Department of Defense. It focuses on emerging operational

[1] Colin Gray, *Another Bloody Century*, (2005), p. 43.

challenges that will impact the conduct of joint warfare in 2035. Its joint nature and ability to consider issues beyond the current Program Objective Memorandum support the Chairman's efforts to initiate a broad conversation about the future of conflict and what that future means for the Joint Force.

The story of future conflict and war found in this document is intended to provide an impartial perspective from which to develop future military capabilities that together can successfully address a range of U.S. security interests. A neutral view does not, however, imply an academic or dispassionate view of the threats, challenges, and opportunities found within the future security environment. Rather, this vision of future warfare is articulated and framed from a U.S. viewpoint and, as such, reflects the concerns, perspectives, and interests of a global superpower with a wide range of global strategic goals.

It is natural that a document such as *JOE 2035* focuses more on how the United States might counter, mitigate, or avoid security challenges as opposed to how the United States might capitalize on emerging opportunities over the next two decades. While the world will certainly see many positive and encouraging changes between now and 2035, the Joint Force must remain alert to potential threats so it can effectively develop and apply military power to defend the United States. However, the vigilant and guarded view of the future security environment found here should be balanced by the recognition and appreciation of promising opportunities available to the United States, its allies and partners, and the Joint Force.

Acknowledgements

JOE 2035 has been enriched by frequent and sustained collaboration with other efforts focused on communicating their own unique part of the futures story. These partnerships began with the National Intelligence Council's *Global Trends* project and the Joint Staff J-5's *Joint Strategic Review* which each helped to shape and inform the strategic context underpinning the operational-level challenges described here. *JOE 2035* has also leveraged the Defense Intelligence Agency's *Joint Strategic Assessment,* the Joint Staff J-3's *Strategic Multilayer Assessment*, OSD's *Project Minerva,* and a range of analytic studies conducted by the National Defense University and its faculty.

JOE 2035 relies on a variety of partners to understand emerging security challenges. This involves ongoing collaboration with the Service War Colleges, which included co-sponsoring the *2014 Army Strategy Conference*. Furthermore, this document was also informed by Service deep-futures efforts, including key documents such as the U.S. Army's *Operational Environments to 2028,* the *Air Force Strategic Environment Assessment 2014-2034,* the U.S. Navy's *Cooperative Strategy for 21st Century Seapower,* and the *Marine Corps Security Environment Forecast 2030-2045.*

Key insights in *JOE 2035* also emerged from persistent engagement and collaboration with a variety of multinational allies and partners. Specifically, *JOE 2035* was informed and influenced by NATO's *Strategic Foresight Analysis* project, the United Kingdom's *Global Strategic Trends* and *Future Operating Environment* documents, Australia's *Future Operating Environment 2035,* France's *Conflicts in the Next Fifteen Years* study, and Germany's *Security Policy and the Future of the Bundeswehr* white paper.

Organization

JOE 2035 consists of three sections that align to the three foundational questions set out in the purpose (see Figure 1).

- ***Section 1: The Future Security Environment 2035.*** This section identifies how emerging trends in three areas – *World Order*, *Human Geography*, and *Science, Technology and Engineering* – may lead to new and challenging conditions that will redefine the security environment of 2035.

- ***Section 2: Contexts of Future Conflict.*** This section explores how the trends and conditions described in section 1 will interact, intersect, compound, or amplify one another to create specific *Contexts of Future Conflict*. Each context illustrates the character of conflict in 2035, the nature of potential adversaries, and the evolving military competitive space.

- ***Section 3: Implications for the Joint Force.*** This section identifies the scope and scale of evolving Joint Force missions. These missions are derived from the intersection of the *Contexts of Future Conflict* described in section 2 with a range of enduring U.S. strategic goals and their associated military tasks.

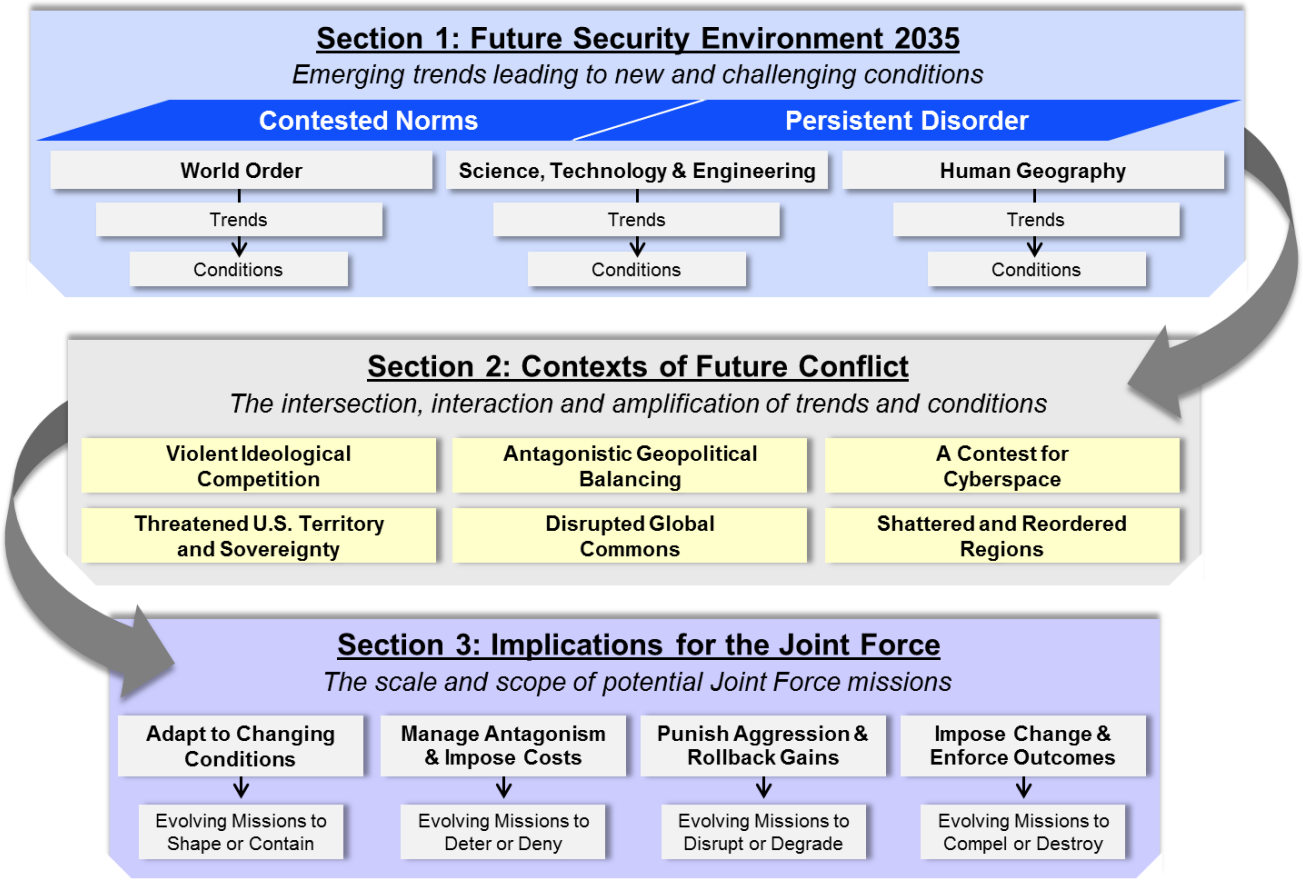

Figure 1. The Organization of *JOE 2035*.

Section 1 - The Future Security Environment 2035

> *"The first, the supreme, the most far-reaching act of judgment that the statesman and commander have to make is to establish . . . the kind of war on which they are embarking."* [2]

The emerging security environment can be described by two distinct but related sets of challenges. The first is *contested norms*, in which increasingly powerful revisionist states and select non-state actors will use any and all elements of power to establish their own sets of rules in ways unfavorable to the United States and its interests. The second is *persistent disorder*, characterized by an array of weak states that become increasingly incapable of maintaining domestic order or good governance. These twin challenges are likely to disrupt or otherwise undermine a security environment that will remain largely favorable to the United States, but less overtly congruent with U.S. interests.

Contested norms and *persistent disorder* are not mutually exclusive. They frequently intersect and involve competition with a military dimension short of traditional armed conflict. This competitive behavior is characterized by ambiguity regarding the nature of a particular conflict, opacity of the parties involved, or uncertainty about relevant policy and legal frameworks.[3] In light of these changes, the ambiguous but still violent pursuit of political goals will be a normal and recurrent condition under which the Joint Force will interact with any number of potential opponents over the next two decades.

What follows is a description of how *contested norms* and *persistent disorder* will manifest in the future security environment across three thematic areas – *World Order*; *Human Geography*; and *Science, Technology, and Engineering*. Within each of these areas, there are a number of conditions that will define and shape the future of conflict and war. Each condition encapsulates three or four militarily-relevant trends that describe the speed and direction of important changes in the security environment. The conditions are designed to provide a "snapshot" of the most critical security-related challenges that the Joint Force will likely confront in 2035.[4]

The first thematic area – *World Order* – describes how the international system may change in terms of state behavior, interstate relationships, and the network of rules, norms and agreements (both tacit and explicit) that govern these relationships. The second thematic area– *Human Geography* – describes the quantity, characteristics, and distribution of human populations around the world and how changing demographics and culture may affect the future security environment. The third thematic area – *Science, Technology, and Engineering* – illustrates a set of likely technological advances and other scientific capabilities that may emerge over the next 20 years to impact the future security environment.

---

[2] Carl Von Clausewitz, *On War*, (trans. Paret and Howard, 1976/1984) p. 88.

[3] United States Special Operations Command, *The Gray Zone* (9 September 2015), p. 1, and Michael Mazarr, *Mastering the Gray Zone*, U.S. Army War College (December 2015).

[4] This section of *JOE 2035* was derived from a Joint Staff J-7 study titled *Anticipating the Future Security Environment: Key Conditions for Future Joint Force Operations* (May 2015).

World Order and the Future Joint Force

International relations are distinct in that it is the only form of social relationship where violence is commonplace and considered in some sense "normal."[5]

Figure 2. Conditions in World Order

The Joint Force will face a future world order largely defined by the conditions listed in Figure 2. Over the next two decades, many of the rules and norms governing the international system will come increasingly under pressure. In a world with no overarching global authority, rules are only as strong as the willingness of states to follow or enforce them. Some rising powers will be dissatisfied with the ability of international institutions to accommodate their growing power and influence. Furthermore, they will strive for the political will, economic capacity, and military capabilities to compel change at the expense of the United States, its allies, partners, and global interests. Other declining, though still powerful, states will seek to insulate themselves from international norms and rules in order to create the political space necessary to threaten and coerce neighbors.

Shifting Strategic Relationships

A combination of more capable competitors, more dangerous threats, and greater fiscal uncertainty is likely to make unilateral action by the United States more difficult and potentially less effective in 2035. Therefore, the United States will continue to pursue collective security arrangements with a large set of capable and often ideologically or culturally compatible actors. While the strategic importance of these relationships is likely to grow, diverse changes will make them more difficult to manage and operate.

Shifting strategic relations among a range of international actors are likely to result from several important trends:

- ***New poles of economic power.*** Some emerging economies in the developing world are gaining relative to Western economies, to include that of the United States, its traditional European partners, and Japan. As a result, a multipolar arrangement might emerge where several states of comparable economic power continually maneuver for advantages over their competitors.
- ***Rebalanced energy security.*** Large increases in economically viable and proven hydrocarbon reserves, increasingly accessible through technological advances such as fracking, will continue to place sharp, downward pressure on energy prices. However, many importers, particularly in East Asia, will struggle to secure access to energy resources through reliable transportation and distribution networks.
- ***The weakening of traditional U.S. alliances.*** Demographic and fiscal pressures will continue to challenge NATO's capacity and capability. Some adversaries may attempt to exploit perceived fractures within the alliance. In Asia, perceptions of reduced U.S. commitment may

[5] Raymond Aron, *Peace and War: A Theory of International Relations* (1967), p. 190.

encourage current allies and partners to pursue unilateral military modernization efforts or explore alternative alliances and partnerships.

- ***The emergence of new partnerships.*** Many nations, including the United States, may turn to "nontraditional" partnerships with a wide array of actors to include self-governing ethnic groups, non-governmental organizations, multinational corporations, and perhaps even friendly local militia groups. The search for unanticipated and atypical partners will likely be a common theme, particularly in the early phases of future conflicts.

In an increasingly multipolar world, the United States is likely to encounter potential adversaries with the capacity to devote significant resources to military spending and the development of their own security partnerships. However, with energy prices expected to remain low for the foreseeable future, many producers will be unable to exercise as much political and financial leverage over energy-poor states. The rise of regional competitors and their network of security partnerships will likely increase friction within existing U.S. alliances and partnerships. Continued U.S. support of allies and partners might antagonize regional powers causing them to undertake efforts to separate local rivals from the United States. Conversely, any perceived U.S accommodation of competing great powers may drive away allies and partners as they no longer view the United States as reliable.

Powers Pursuing Regional Primacy

In the future, some states will increasingly use coercion and force to change regional arrangements in their favor. Potential adversaries able to avoid or protect themselves from U.S. power projection will gain the freedom of action to shape the behavior of their regional neighbors, sometimes through violence and coercion. This pressure is likely to take place through large scale conventional overmatch against local rivals combined with cost-imposing niche capabilities to deter U.S. intervention. The ability to hold high-value assets or critical infrastructure at risk may constrain U.S. involvement and improve the prospects for successful coercive strategies at local or regional levels.

The willingness and ability of certain powers to seek regional primacy is likely to result from several important trends:

- ***The refinement of state hybrid stratagems.*** A number of revisionist states will employ a range of coercive activities to advance their national interests through combinations of direct and indirect approaches designed to slow, misdirect, and blunt successful responses by targeted states. These hybrid stratagems will be designed to spread confusion and chaos while simultaneously avoiding attribution and potentially retribution.
- ***The intensification of warfare by proxy.*** Proxies will continue to offer political and economic advantages such as minimizing the risk of escalation, providing plausible deniability, and avoiding the costs of direct involvement. Furthermore, shifting alliances and partnerships of convenience will make it difficult to distinguish who is involved in a conflict, what interests they represent, and why they are fighting.
- ***The establishment of regional nuclear deterrents.*** The next two decades may feature competitors that pursue a rudimentary nuclear capability to establish a credible nuclear deterrent. Some states may attempt to "break out" of the Non-Proliferation Treaty regime and deploy dozens to hundreds of nuclear weapons on a range of delivery platforms such as ballistic missiles, submarine launched cruise missiles, or portable, miniaturized weapons.

A hybrid mix of conventional deterrence and proxy warfare will challenge the ability of the Joint Force to intervene successfully in support of allies and partners targeted by nearby, revisionist powers. The core attributes of state hybrid stratagems will be "…characterized by convergence [of] physical and psychological, kinetic and non-kinetic, combatants and noncombatants…" and the operational fusion of conventional and irregular approaches.[6] It is likely that Russia will continue to use the threat of military power to secure regional interests and promote perceptions that it is still a great power. Iran will continue to develop and leverage regional proxies and partners. Meanwhile, China might develop a more dynamic and adaptive maritime stratagem in an attempt to impose irreversible outcomes for island disputes in the East and South China Seas.

Regional Powers Attain Global Reach

Should competitors consolidate a measure of regional primacy, the next logical step will be to invest in the capabilities necessary to assert themselves even farther from their borders both globally and across regions. The leading edge of this new global reach will be investments in more advanced cyber capabilities. Strategic attacks will likely focus on disrupting elements of the U.S. financial infrastructure, where trust and data integrity are paramount. Furthermore, U.S. energy infrastructure, dependent on industrial control computers, might also be a focus for adversary cyber activities. Additionally, a wider and more capable array of missiles, aircraft, surface vessels, and subsurface platforms will extend the physical reach of some powers.

Regional powers attaining global reach is likely to result from several important trends:

- ***Increased competition across the air and maritime domains.*** Some states will assert their own divergent views about access to and use of the air and maritime commons. This will most likely occur within 12 to 200 nautical miles of coastlines as some competitors establish new Air Defense Identification Zones (ADIZ) and continue to obstruct the innocent passage of reconnaissance and military patrols through their Exclusive Economic Zones (EEZ).
- ***Emergence of new spacefaring nations and military competition in space.*** Many capabilities previously reserved to superpowers are now available to other states on a commercial basis, to include Earth observation, optical sensing, space-based Internet, and communications services. A range of anti-satellite weapons (ASAT) able to disrupt or destroy the space, electromagnetic, and ground segments of these constellations will also become more common.
- ***Growth of state-sponsored cyber forces and capabilities.*** The next decades will see the further emergence of state-sponsored actors and associated organizations with more advanced cyber warfare capabilities. Like strategic airpower before it, state-based cyber advocates will develop strategies that attempt to "leap over" traditional U.S. military forces and directly influence the decision calculations of political and military leadership.

The emergence of regional powers with a measure of global reach may cause the United States to divert a greater portion of scarce defense resources toward direct homeland defense capabilities (for example, more extensive air and missile defenses) at the expense of global power projection capabilities. Furthermore, a demonstrated ability to hold the U.S. homeland at risk may be part of larger strategies to discourage the United States from intervening in support of allies, partners, or other global interests. Future competitive great powers will be active all over the globe, and these

[6] Frank Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* (2009), p. 34.

highly connected and globally-present states will make containment, isolation, and blockade operations increasingly difficult.

Evolving Roles of International Institutions

A number of states around the world are investing in new political, economic, and security arrangements to reflect their growing power and confidence. Fundamental differences with regard to natural resource issues, human rights, and responsibilities in the maritime, air, space, and cyber domains will prevent existing global governance frameworks from adequately managing some emerging security challenges. While most rising powers are likely to focus on gaining greater access and influence within the current international system, some states will be willing to use violence or coercion to revise certain aspects of the international order.

The evolving role of international institutions is likely to result from several important trends:

- ***Contested international rules.*** Rising powers including for example, China, Russia, India, Iran, or Brazil have increasingly expressed dissatisfaction with their roles, access, and authorities within the current international system. The inability or unwillingness to accommodate the aspirations of these powers in the future may increasingly cause some states to challenge or even reject current rules and norms.
- ***Erosion of standing institutions of international order.*** Tension between individual states pursuing their interests alone and the reflex to subsume some of those interests in pursuit of common goals is likely to intensify. Without an overriding sense of common purpose, states may be less willing to support collective efforts through standing international organizations that make and adjudicate the rules underpinning a secure and stable international order.
- ***Emergence of alternative institutions of international order.*** The use of financial instruments of power by the West to disconnect revisionist states will increase their incentive to pursue alternative political and economic arrangements. For example, a future Shanghai Cooperation Organization (SCO) could represent up to half of the world's population, 35 percent of global economic output, and account for nearly 20 percent of the world's oil production.

The United States is likely to confront a future security environment in 2035 where it could be forced to contend with new and broadly legitimate international rules and agreements that it had little part in making. Increased competition over international rules will be most apparent in instances where they are poorly defined, such as the nature of EEZs, and ADIZs, and the use of outer space and cyberspace for economic and military purposes. Furthermore, a number of states will chafe against international agreements that they perceive to levy different (and unfair) rights and responsibilities on states such as the Nuclear Nonproliferation Treaty (NPT) or Intermediate Range Nuclear Force (INF) Treaty. This promises to increase the potential for dangerous and unstable arms-racing behavior among military competitors.

Connected Consequences of Fragile and Failing States

There will be additional instances of weak states becoming failed states in the future. While the specific circumstances behind each failure will differ and include a mix of real or perceived corruption, economic inequality, and ethnic/religious discrimination, the root cause of these conflicts will often be traced to the inability or unwillingness of central governments to provide effective and legitimate governance. Consequently, as internal authority is challenged and begins to collapse, violence is likely to occur in the form of sectarian strife, insurgency, or civil war.

The broad and dangerous consequences arising from fragile or failing states are likely to result from several important trends:

- ***Continuing internal collapse of weak states.*** Some central governments will find it increasingly difficult to maintain power and control over their populations as groups object to mistreatment and neglect. While some disenfranchised sub-state actors will have legitimate grievances, other groups will exploit failures by the central government as a justification to seize more power, important resources, or strategic territory.
- ***Fracturing of weak states by external powers.*** The steady erosion of the willingness and ability of some states to prioritize other states' sovereignty over other issues is likely to continue into the foreseeable future. Certain revisionist states are likely to view the fracturing of weaker states as an expedient way to change various regional balances of power in a manner unfavorable to U.S. interests.
- ***Uncontrolled spread of weapons of mass destruction.*** It is likely that terrorist, insurgent or criminal groups will eventually obtain chemical, biological, radiological, or even nuclear weapons within the next two decades. While they might develop WMD by converting commercially available materials, a more likely possibility is the seizure of weapon stockpiles in a fragile state that can no longer maintain positive control of its arsenal.
- ***Inability to contain infectious disease.*** There is likely to be a steady rise in the incidence and severity of infectious disease outbreaks. While even relatively strong and stable states may struggle to respond to pandemics, weak states will confront significant challenges containing outbreaks due to inadequate surveillance and early warning, weakened public health systems, and the absence of trained doctors and nurses.

As states erode and fail, the danger is not simply the potential for adverse effects at the local level, but more importantly for the United States, what their collapse does to the broader world. Failing states create dangerous, transregional ripples with other, long-term global consequences. For example, non-state actors may acquire and employ chemical, biological, radiological, or nuclear weapons in unexpected and unrestrained ways designed to inflict the greatest damage possible against the United States and its allies. Furthermore, the inability of weak states to effectively respond to epidemics may require external intervention in order to contain and prevent the global spread of infectious diseases.

Human Geography and the Future Joint Force

> *"Time and again it has been in the wake of the decline of empires, in contested borderlands, or in power vacuums, that the opportunities have arisen for genocidal regimes and policies. Ethnic confluence, economic volatility, and empires on the wane; such was and remains the fatal formula."*[7]

The Joint Force will face a future socio-cultural world largely defined by the conditions depicted in Figure 3. The future security environment will feature large areas of the globe where states struggle to maintain a monopoly on violence and individual identities are no longer based exclusively on a sense of physical location. Individuals and groups will connect and socialize globally. Widespread economic growth will raise millions out of poverty into longer and more comfortable lives. However, a richer human world lacking legally constituted and legitimate governance may lead to dissatisfaction, violence, and even the emergence of violent transnational ideologies that disrupt local, state, or regional governments. Growing wealth can also stress food, water, energy, and other resources, causing higher prices and shortages which may translate into instability, civil conflict, and the failure of governments. Fractured and failed governments may transmit disorder more broadly or become geopolitical opportunities for more well-ordered and aggressive states.

Figure 3. Conditions in Human Geography

Intensifying Consequences of Population Growth and Migration

By 2035, the global population is expected to increase by another 1.8 billion people to a total of nearly 9 billion people, with almost all of this growth occurring in the developing world and largely centered in urban areas. When properly harnessed, population increases and urbanization can translate into stronger economic development and expansion. However, massive population growth and migration might stress governments to the breaking point where they are unable to effectively manage resources and meet their citizens' basic needs. Unequal rates of economic growth and the lack of opportunity are already inducing unexpected migrant flows, stressing recipient states and limiting the prospects for growth and development in places they leave behind.

The intensifying consequences of population growth and migration are likely to result from several important trends:

- ***Asymmetric population growth patterns.*** The center of gravity for the world's population continues to shift from the developed world to the developing world. The highest growth in population is likely to occur in Africa, while the populations of most countries in South Asia and the Middle East are expected to continue rising, with India surpassing China as early as 2022 as the most populous nation on Earth.
- ***Mass migration and irreconcilable immigrants.*** The mixing of new people, ideas, culture, and ideologies can result in unrest and conflict between those moving in and native citizens.

[7] Niall Ferguson, *The War of The World*, (2006), p. 646

Many receiving nations will be incapable of integrating new immigrants, which might lead to disenfranchised, insular immigrant communities and the broader emergence of politically irreconcilable and potentially violent insurgent groups.

- ***Mass migration and rejected immigrants or minorities.*** As more immigrants enter more countries around the world, they are likely to demand political representation. However, some states will be unwilling to accommodate new immigrants and risk inciting unrest among local populations tiring of immigrant demands. This unwillingness to assimilate immigrants might cause some to become resentful of perceived failures by the host society.

The future security environment is likely to feature large, culturally unassimilated urban enclaves and physically isolated refugee camps in many regions of the world, where immigrants often have profound cultural, religious, and economic differences from the indigenous populations. Some immigrants entering a country may disrupt areas within their host society if they are not treated equally or perceive they are being treated unequally. Conversely, tension between the aspirations and goals of majority and minority populations might ultimately cause the majority population to become hostile and apply terror, violence, or other coercive instruments of the state against minority populations. The resulting instability, strife, and conflict is likely to lead to even greater migration as refugees flee to better-governed or more economically viable areas of the world. Ultimately, this may imply a future with more walls and barriers, frequent offshore patrols by maritime agencies and navies, and intrusive surveillance operations designed to better control and manage the flow of migrants.

Urban Concerns as Global Security Issues

Humanity is now a predominantly urban species. Urbanization will likely continue to increase into the foreseeable future, with some 60% of the global population living in cities, usually near oceans, by 2035. The pace of urbanization is expected to be the fastest in lower-middle income countries. Many cities are likely to see significant and consequential economic, political and social advances. However, some cities will struggle to cope with the challenges posed by poverty and inadequate or aging infrastructure. Paradoxically, the adoption of information technologies will outpace the provision of adequate transportation, sanitation, and other necessities, leaving poor urban areas as heavily instrumented and connected to the global information environment as today's most developed cities.

The increased importance of urban security issues in the future security environment is likely to result from several important trends:

- ***Demand for food or water exceeding local capacity to affordably deliver.*** Demand for supplies of food and water in the developing world will continue to increase. Many nations depend on the largesse of oil-rich patrons or state-owned domestic oil companies to maintain their fiscal solvency. However, fiscal imbalances could prevent these states from meeting payment requirements in order to maintain adequate subsidies.
- ***Expansion of under-governed urban spaces.*** The continued rapid and unplanned growth of many urban areas is straining the ability of local governments to provide adequate services, governance, and security. These poorly governed urban zones are more likely to permit the development of black markets, which facilitate the illicit flow of goods, currency, and human trafficking.

- ***Emergence of global cities as international actors.*** As urbanization continues to proceed globally, it will likely be accompanied by the continuing rise of global cities as centers of power, sometimes influencing their host nations – and at times transcending them altogether. As global cities develop greater economic and demographic power, people may associate their identity more closely with their city rather than their country of residence.

Urban environments will remain an extremely challenging location for the Joint Force to operate. Alienation, poverty, and disorientation of formerly rural residents interacting with more cosmopolitan urban citizens may increase the potential for criminal and gang-related activities as well as the development of urban insurgent groups. These adversaries will use urban areas to negate U.S. standoff reconnaissance and strike advantages by creating sheltered locations hidden within urban clutter. The Joint Force will either fight or attempt to contain adversaries within and across urban agglomerations that sprawl over hundreds of square miles, are located in littorals, and contain tens of millions of people. They will typically feature subterranean infrastructure, shantytowns, and skyscraper canyons in varying states of functionality and disrepair. This built-up environment can degrade or reduce mobility as well as the effectiveness of advanced weapons, communication systems, and intelligence, surveillance, and reconnaissance (ISR) capabilities.

Evolving Ideological Conflict

Identity is defined as the set of characteristics by which a person is recognizable or known. Humans define their identity in many ways, including religion, ethnicity, race, language, gender, tribe, class, occupation, geography, and nationality. Increasingly permeable national borders mean that human society will discover many more ways for ideas, images, narratives, and messages to propagate in in the future. However, more contact between cultures is just as likely to result in negative consequences as positive. People of all cultural and ideological persuasions are frequently repelled or even disgusted by new ideas, cultures, or customs as opposed to being attracted by or inquisitive of them.

Evolving ideological conflict is likely to result from several important trends:

- ***Declining legitimacy of state authority.*** Under pressure from internal corruption or external stressors, state authorities in many parts of the world will be unwilling or unable to provide the level of support their citizens expect. This mismatch between relatively well-off state authorities and those displaced and disrupted by globalization or other shocks will result in strife and conflict.
- ***Rapidly shifting group identities.*** Group identities will likely change rapidly in the future as the speed and capabilities of information technologies increase. Advanced information technologies will lead to new and faster ways to form, build, and maintain cohesion and common purpose among members of a group. Consequently, it will become easier to mobilize and expand groups and ideas, irrespective of geographic proximity.
- ***Increasing ideological polarization.*** Transnational ideological bonding and/or repelling will create significant barriers to critical discourse and perpetuate a lack of understanding and empathy for alternative beliefs, values, and norms. Groups that fit comfortably within a single political entity may, through increased polarization, no longer have the capacity to resolve differences through common political processes.

Shifting ideological affiliations could lead to new and surprising fractures in societies. Rapidly shifting groups may mobilize populations by encouraging greater intolerance, prompting urban political paralysis, and orienting their members on radical but still coherent violence in the service of political ends. Terrorists, insurgent groups, and state-sponsored proxies are likely to take advantage of a range of polarization techniques to reinforce their messages or to create favorable conditions within which to operate. This environment will ultimately lead to new forms of "shadow" governance where organizations the United States deems illegal or illegitimate begin to fulfill citizens' needs – and problematically, are seen as legitimate by the local population. These groups will build regional and global networks around sets of ideas, forged and disseminated within cyberspace, with a range of "online ideologies" and identity networks displacing nationalism as a source of legitimacy for many.

Alternative Hubs of Authority

Over the next two decades, the distribution of power will continue to transition away from a state-centric world towards a multi-level, multi-nodal model, characterized by competition for control and influence between different institutions, groups, and individuals. By 2035, varying kinds and degrees of economic, informational, and ideological power will be exercised by non-state actors such as non-governmental organizations (NGOs), private corporations, extremist groups, or empowered individuals that may include celebrity figures and the wealthy. As a result, formal governing organizations and mechanisms within states will become increasingly less effective, while informal networks will increase their capacity and capability to control or drive international and domestic outcomes.

The emergence of alternative hubs of authority is likely to result from several important trends:

- ***An accelerating diffusion of power.*** The power of the state is likely to be eroded by an array of non-state actors who will be increasingly capable of distributing and diffusing control over outcomes away from states at global, national, and local levels. Future conflict will involve a greater number of actors, both state and particularly non-state entities, due to a continuing diffusion of power.
- ***Cooperation/convergence among terrorist and criminal organizations.*** Despite differing goals and objectives, terrorist groups and criminal organizations will converge at times to plan or complete a particular operation of common interest. Dependent on very local conditions, the linkage between criminal and terrorist groups is likely to increase in both geographic terms and in terms of specialization such as logistics, finance, and security.
- ***Globalized criminal and terrorist networks.*** Technology designed to maintain anonymity such as The Onion Router (TOR) or the Invisible Internet Project (I2P) as well as improved encryption techniques will allow illicit networks to evade detection and expand operations. Globalized criminal and terrorist entities are likely to amass significant financial resources and demonstrate the ability to challenge traditional state economic and military capabilities.

Future conflict will center on an array of organizations filling spaces vacated by states. Some terrorist organizations will leverage and exploit illicit activities such as drug smuggling, human trafficking, and even poaching to develop new lucrative sources of funding for their violent activities. Conflict resulting from a more integrated criminal-terrorist group nexus will not necessarily lend itself to a purely military solution, as financial flows and movement across many legal jurisdictions transcend military boundaries and authorities. As the line between terrorist and

criminal activities continues to blur, the transactional connections between a wide-range of unlawful organizations is also likely to blur the distinction between law enforcement and military operations. The Joint Force may find it more difficult to distinguish between allies and adversaries, and determine who really matters, who to engage, and who to support.

The Rise of Privatized Violence

States will find it increasingly difficult to maintain a monopoly on the use of force. Private and non-state groups, in the absence of strong or legitimate states, will increasingly turn to violence to advance their political, social, ideological, or economic goals. Sub-state and transnational actors will be enabled by the ability to rapidly share information through mobile devices and associated social media platforms. Collective action and popular movements, which once took once took months or years to build, will be catalyzed in hours. Small determined groups or even lone radicalized individuals will continue to wield enormous influence using "off grid" mesh networks to disrupt the political and social order of a nation.

The rise of privatized violence is likely to result from several important trends:

- ***Adaptive irregular/sub-state adversaries.*** Adversaries will continue developing capabilities to avoid or withstand U.S. technological overmatch. Many criminal and terrorist groups are likely to combine relatively cheap, accessible, and potentially disruptive technologies – such as social media, smartphones, 3D printing, robotic and autonomous systems – to degrade or even defeat U.S. systems in the future.
- ***Disruptive manufacturing technologies and the urban arsenal.*** The proliferation of technology and a wide range of manufacturing capabilities in many urban areas will likely continue over the next two decades and might lead to novel advances, to include pervasive intelligence, surveillance, and reconnaissance instruments and relatively cheap and simple, yet effective strike assets such as 3D printed drones or sophisticated IEDs.
- ***Weaponization of commercial technologies.*** Over the next two decades, a greater number of people will become connected and begin to take advantage of mobile technologies. Driven largely by expected advances in computerization, miniaturization and digitization, potential adversaries will likely have greater access to more sophisticated weaponry that does not require sophisticated users to effectively employ.

Transnational criminal organizations, terrorist groups, and other irregular threats are likely to exploit the rapid spread of advanced technologies to design, resource, and execute complex attacks and combine many complex attacks into larger, more sustained campaigns. Potential adversaries might leverage commercially available cell phone and networking capabilities to issue real-time propaganda through social media that portrays the Joint Force in a negative manner and highlights actual or perceived injustices. Or, the Joint Force might be confronted by a more lethal battlefield as potential adversaries use basic but effective strike assets to impose significant costs on units conducting urban combat operations. However, in the future the Joint Force could leverage technology to disrupt, deny, and defeat these systems, using many of the same asymmetric techniques that adversaries currently employ against the United States.

Science, Technology, and Engineering and the Future Joint Force

> "*The future of warfare is not synonymous with future technology, but warfare must always have a technological dimension."*[8]

The Joint Force will face a future technological landscape largely defined by the conditions depicted in Figure 4. The U.S. approach to high-technology warfare over the past two decades has encouraged the development of asymmetric, unconventional, irregular, and hybrid approaches by adversaries. Adversaries will continue to innovate by applying varying mixes of high and low technologies to frustrate U.S. interests and military forces. By 2035, the United States will confront a range of competitors seeking to achieve technological parity in a number of key areas. Adversary forces will be augmented by advanced C3/ISR and information technologies, lethal precision strike and area effect weapons, and the capacity to field first-rate technological innovations. The cumulative result will be a situation in which, "*Our forces face the very real possibility of arriving in a future combat theater and finding themselves facing an arsenal of advanced, disruptive technologies that could turn our previous technological advantage on its head – where our armed forces no longer have uncontested theater access or unfettered operational freedom of maneuver.*"[9]

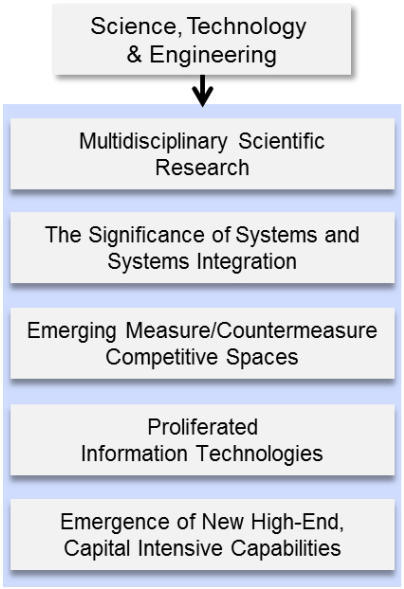

Figure 4. Conditions in Science, Technology & Engineering

Multidisciplinary Scientific Research

By 2035, many important scientific advances will result from an emphasis on how differing phenomena interact and how seemingly diverse technological domains relate to one another. They will frequently take place where two or more disciplines converge, particularly in the rapidly evolving areas of biology, robotics and autonomy, information technology, nanotechnology, and energy.[10] Many consequential technological changes are less likely to emerge from a Department of Defense lab or single research institution, but from ongoing work across clusters of collaborative research and development efforts – typically geographically dispersed and sometimes international in nature.

This evolving approach to fundamental scientific research is likely to result from several important trends:

- ***Applied metamaterials.*** Metamaterials are manmade, three-dimensional composite materials that reliably manipulate electromagnetic radiation. Widespread metamaterial applications will

[8] Colin Gray, *Another Bloody Century*, (2005), p. 98.
[9] Deputy Secretary of Defense Robert Work, Remarks to the National Defense University Convocation (August 5, 2014).
[10] National Defense University has described the potential for high-impact technological change as occurring along five major themes: Biology, Robotics, Information Technology, Nanotechnology and Energy (or BRINE). James Kadtke and Linton Wells II, "Policy Challenges of Accelerating Technological Change: Security Policy and Strategy Implications of Parallel Scientific Revolutions," National Defense University, Center for Technology and National Security Policy, p. 1 and 7.

lead to new means of signature control, the development of low-probability intercept active sensors, the application of high-resolution planar lenses, and the use of compact antennas.

- ***Exploitation of unique material properties at the nanoscale.*** The ability to make and modify materials at the nanoscale will allow manufacturers to take advantage of many new properties. Anticipated advances in nanomaterial technologies (combined with parallel improvements in metamaterials) suggest that more complex composites and bespoke materials will emerge with properties engineered precisely to optimize performance.
- ***Fuels and batteries with increased energy density.*** Advances in energy systems (particularly those based on hydrocarbons) will likely be evolutionary, and expected improvements in energy density may enable advances in directed energy weapons, increase the loiter time of unmanned vehicles, lead to more effective sensors, and reduce the size and weight of man-portable systems.
- ***Biochemistry and biological engineering*.** New techniques to edit and modify the genome may allow scientists to harness organisms or biological systems as weapons or to perform engineering tasks typically impractical with conventional methods. Future advances might include the construction of new biological parts, brain-computer interfaces, or the re-design of natural biological systems to manufacture drugs, chemicals, materials, or food.

Economic and military advantages will accrue to those nations with dense university clusters, a community of businesses that transform primary research into usable prototypes, and education systems that encourage collaboration, experimentation, and innovation. Furthermore, because research clusters are frequently international in nature, novel scientific advances may not be claimed by single nations. The United States must focus on understanding the areas that research clusters are investigating and be willing to explore how the application of multidisciplinary scientific discoveries might augment and upgrade (or erode and obsolesce) its current portfolio of capabilities. Future force development activities must be capable of interacting with research clusters, and encouraging these clusters to research technologies that may lead to distinct U.S. military advantages.

The Significance of Systems and Systems Integration

The corollary to change in multidisciplinary basic research at the engineering level is the importance of systems integration to make emerging technologies economically or militarily useful. Effective technology integration into military operations requires the capacity to bring together many different capabilities into a coherent, purposeful whole. Even today, the largest, most capable states struggle to match their ability to develop individual technologies with the ability to integrate these technologies into a single system. By 2035, improvements to individual devices, tools, or platforms will likely become less important than the system architectures which allow dissimilar capabilities to work together coherently.

The significance of systems and systems integration is likely to result from several important trends:

- ***Additive manufacturing goes global.*** Additive manufacturing processes in both the commercial and government sectors will likely grow and proliferate to an array of competitor states, terrorists, and criminals. These capabilities will permit the mass customization of parts, the development of lighter and stronger components, the use of rapid reverse-engineering, and a reduced need for expensive and vulnerable supply chains and warehousing facilities.

- ***Evolution of autonomous robotic systems.*** The next two decades will see significant advances in autonomy and machine learning, to include the emergence of robots working together in groups and as swarms. New and powerful robotic systems will be used to perform complex actions, make autonomous decisions, deliver lethal force, provide ISR coverage, and speed response times over wider areas of the globe.
- ***Open source design.*** Greater connectivity between states, groups, and individuals will facilitate more sharing of ideas and designs, which users can then modify, change, or otherwise improve to optimize them for their own purposes. By 2035, a new shared design "ecosystem" may evolve to provide a wide range of customizable plans for a range of hardware, to include defense and military applications.
- ***Emergence of micro/nano-satellites and near-space capabilities.*** Micro/nano-satellites, as well as ultra-high altitude aircraft and balloons, will continue to replace large satellites because they are considerably cheaper and faster to build and launch. These advances will likely lead to improved reliability, with networks of small satellites and stratospheric swarms performing the tasks previously reserved exclusively for large satellites.

In 2035, military advantages will not only be derived from a single technology but also from the integration of many technologies in systemic and coherent ways. For example, the (now) rapid advance of self-driving cars is as much about the wide availability of cheap GPS and high-quality terrain maps as it is the development of on-board environment sensing capabilities. This suggests the need to better integrate geospatial data with military robotic systems in the future. Furthermore, rather than civilian "spin-off" applications from military research and development efforts, military technological change will be "spin-on" as advances come from civilian and foreign investments in technologies for non-military purposes. The disruptive potential of this development will fully emerge when adversaries begin to experiment with the design, construction, and speedy refinement of a range of IEDs, drones, firearms, or other weapons.

Emerging Measure/Countermeasure Competitive Spaces

Technological change will result in new types of competitive interactions among military forces. The most pressing of these will be the contest of "hiders" vs. "finders" on the battlefield. Adversaries will continue to offset U.S. airpower and other long-range strike advantages by developing well-protected underground facilities, hardened fiber optic networks, and numerous high quality decoys, both virtual and physical. They will also focus on developing long-range strike capabilities and an evolving array of sensor and missile technologies to limit U.S. power projection capabilities. Regional reconnaissance-strike complexes will target the expensive, few, and/or easily locatable bases and platforms upon which current U.S. forward presence relies.

Evolving measure/countermeasure competitions are likely to result from several important trends:

- ***Proliferation of advanced radio-frequency weapons.*** Advances in phased-array technology will facilitate the development of beam-focusing systems, which will permit high-powered radio frequency (HPRF) weapons to degrade or destroy very precisely versus omnidirectional systems. This will lead to new applications for area denial, crowd control, and the destruction of a range of electronic equipment
- ***Availability of non-nuclear EMP.*** Non-nuclear electromagnetic pulse (NNEMP) weapons will allow for the discriminate and precise targeting of a range of electronics-based systems. The next two decades will see these weapons integrated into air, ground, and surface systems

providing adversaries the capability to disrupt, degrade, and disable components of U.S. and allied C4/ISR networks.

- ***Robotics as a force multiplier.*** Emerging autonomous robotic systems are being increasingly used to augment, rather than simply replace, individuals and platforms. The augmentation of human systems with robotics, particularly swarming, will permit longer duration missions, enable greater lethality, improve the ability to protect capital platforms from attack, and increase individual human and unit performance.

Advances in electromagnetic warfare techniques will provide new methods to engage the circuitry and software of weapons systems, suggesting the emergence of rapidly evolving sensor/counter-sensor battles. Electronic warfare will be a race won by the force that can swiftly identify, understand, and optimize signals to counter radar and sensor systems. The search for weak signals against cluttered backgrounds will be augmented by enhanced data processing and storage, as well as large scale interpretive computing capabilities. Furthermore, the proliferation of sensors is likely to encourage the development of small and/or stealthy robotic systems that operate below detection thresholds. As industrial-scale robotics manufacturing evolves, future warfare may see a rebalance away from militaries built around the few, expensive, and highly-capable platforms to many, cheap, and "good enough" systems.

Proliferated Information Technologies

Very powerful information technologies will be widely available around the world by 2035, including wireless handheld or even brain-interfaced devices with advanced levels of connectivity. More modern developing states will continue to construct comprehensive national information technology infrastructures consisting of fiber-optic and cellular networks that far exceed the current state of the art. Potential competitors will have access to huge volumes of commercially-available geospatial and other geophysical data that once cost billions and was available to only to the richest and most technically-competent countries.

Proliferated information technologies are likely to result from several important trends:

- ***Regional C3/ISR parity.*** Potential adversaries will likely develop and deploy advanced C3/ISR capabilities that can be coupled to precision and area weaponry. As a range of sensors, information networks, information processing, and data fusion capabilities becomes widely available to potential adversaries from high-end states to lower-end insurgent and irregular forces, U.S. military forces may be identified, tracked, targeted, and attacked at range.
- ***Exploitation of C3/ISR vulnerabilities.*** Technologies that can damage, spoof, confuse, or disrupt integrated battle networks will become increasingly available. U.S. and partner C3/ISR systems will require enhanced system protection, greater network redundancy, and automated defenses capable of reacting in a highly dynamic environment. The Joint Force might also exploit the opportunity to target adversary networks lacking sufficient hardening or protection.
- ***Advanced information analysis and exploitation.*** Growing digital inter-connectedness and the linking of the Internet to the physical world will likely create an 'Internet of Things' which will further increase the amount of information generated, processed, and stored. Future software developments are likely to focus on new algorithms, and optimization techniques will assist in making sense of these large data sets.
- ***Quantum information science.*** The successful development of quantum computers might increase the ability to understand, model, and predict behaviors of very complex systems such

as weather, economics and finance. Additionally, quantum cryptography will lead to new encryption and decryption techniques, which may significantly enhance communications in electromagnetically cluttered or denied environments.

By 2035, people will continue to willingly add significant amounts of their own personal data to public networks, including full-motion video. However, the way information is transmitted, protected – or made vulnerable – will change dramatically. Adversaries will have improved mapping and observation capabilities beyond their borders, and they may have the ability to better understand the basing, disposition, and capabilities of U.S. forces. Biometric identification (perhaps at range) may strip away the anonymity that enables insurgents to blend into a society – or will allow future adversaries to identify, track, isolate, and target individual U.S. political or military leaders. Meanwhile, new data interrogation techniques will enable better understanding of patterns and permit large-scale inferences about the behaviors of societies by analyzing geographic data, purchasing and financial information, and other relevant information.

Emergence of New High-End, Capital Intensive Capabilities

Although cheap, pervasive, and proliferated capabilities such as personal information technologies or small autonomous aerial vehicles attract a great deal of attention, a number of expensive, investment-heavy technologies will emerge by 2035 that may provide significant military advantages. Many of these advanced and highly capable technologies will only be accessible to states with significant financial and scientific resources as well as extensive industrial and manufacturing infrastructure. Thus, the fascination with small and cheap must be balanced against an appreciation for capital-intensive weapons and industrial technologies with the potential to dramatically alter the strategic landscape.

High-end, capital-intensive military capabilities are likely to result from several important trends:

- ***Deployment of >100 KW electrical lasers.*** Electrical laser systems will become smaller, lighter, and cheaper, and the introduction of femto- and pico-second pulses will lead to novel sensors and effects. Ultra-precise, multiple shot, weaponized lasers will easily achieve >100 KW, permitting stealthy engagements at longer ranges with less dwell time required to achieve effects.
- ***Breakthrough energy.*** Many energy development efforts focus on making current systems and processes more efficient, often producing significant but incremental improvements. However, research into groundbreaking technologies has the potential to radically impact the future of energy. Innovative fusion, solar, and biofuel technologies might lead to the development of highly mobile, lighter weight, and more efficient power sources.
- ***Hypersonics.*** It is probable that one or more states will field an operational hypersonic weapon system within the next two decades. Likely to achieve speeds in excess of one mile per second on non-ballistic flight paths, functional hypersonic systems will improve the range, accuracy, and lethality of offensive global strike capabilities and have the potential to disrupt portions of anti-access / area denial capabilities as well as missile defense systems.

New high-end military technologies will likely have the largest and most immediate impact in the air and space domains. As the deliverable power of laser systems continues to increase, they will become extremely useful in denying the air domain to fragile, readily detectable conventional platforms as well as guided and unguided munitions of all types unless effective countermeasure

materials and functions are developed. Furthermore, the combination of advanced power generation and electrical laser systems may provide extensive advantages in controlling the air and sensor battle from low Earth orbit, stratospheric air vehicles, or land / sea platforms. Expensive but powerful compact power generation coupled with new energy management will also potentially enable the use of railguns. Ultimately, the ability to increase the speed of aerospace engagements across the board will present significant challenges, particularly if coupled with the autonomous lethal decision-making capabilities that adversaries are more likely to employ.

Summary

This section described a range of individual trends that will likely converge to produce a set of conditions across *World Order, Human Geography,* and *Science, Technology, and Engineering.* Competitor states and some powerful non-state actors will increasingly challenge the rules that underpin the current global order. Meanwhile, fragile states will become increasingly incapable of maintaining order. Moreover, anticipated scientific and technical advances will likely lead to greater parity among a range of international actors thus allowing potential adversaries to more effectively challenge U.S. global interests. Together, these conditions illustrate *contested norms* and *persistent disorder* in the future security environment.

While it is important to establish a baseline description of the emerging security environment, looking into the future is never this straightforward. The simple identification of trends and resulting conditions is not sufficient to understand the changing character of conflict and explore reasons why the Joint Force might be required to support U.S. interests at home and abroad by addressing *contested norms* and *persistent disorder*. In reality, trends and conditions do not exist independently, but are closely related to other evolving trends and conditions. Sometimes these relationships are clear, but more often, they interact in unanticipated and perhaps surprising ways.

Section 2 explores how the individual trends and conditions described within the three thematic areas – *World Order*, *Human Geography*, and *Science, Technology and Engineering* – may intersect, compound, or amplify one another to create six *Contexts of Future Conflict.* These contexts are a mechanism to illuminate why future conflict and war may occur and to describe the evolving character of conflict in 2035. They are not predictions but instead are designed to assist in "…understanding the potential contours…in which force will be applied and how future adversaries will fight [by examining] myriad combinations that will arise."[11]

[11] Frank Hoffman and Pat Garrett, "The Great Revamp: 11 Trends Shaping Future Conflict," *War on the Rocks* (8 October, 2014).

Section 2 - Contexts of Future Conflict

"Context decodes the origins, meaning, character, and consequences of warfare."[12]

Conflict and war in 2035 cannot be understood by the simple identification of a set of individual trends and conditions. Instead, the intersection and interaction of many discrete trends and conditions will ultimately change the character of future conflict and illuminate the reasons why the Joint Force may be called on to address threats to U.S. national interests. In fact, conflict in 2035 is likely to be driven by six specific and unique combinations of trends and conditions.[13] Each of these *Contexts of Future Conflict* creates a troubling problem space for the Joint Force. They include:

1. ***Violent Ideological Competition.*** Irreconcilable ideas communicated and promoted by identity networks through violence.
2. ***Threatened U.S. Territory and Sovereignty.*** Encroachment, erosion, or disregard of U.S. sovereignty and the freedom of its citizens from coercion.
3. ***Antagonistic Geopolitical Balancing.*** Increasingly ambitious adversaries maximizing their own influence while actively limiting U.S. influence.
4. ***Disrupted Global Commons.*** Denial or compulsion in spaces and places available to all but owned by none.
5. ***A Contest for Cyberspace.*** A struggle to define and credibly protect sovereignty in cyberspace.
6. ***Shattered and Reordered Regions.*** States unable to cope with internal political fractures, environmental stressors, or deliberate external interference.

Each context includes elements of both *contested norms* and *persistent disorder*. However, their relative importance will vary depending on the objectives of potential adversaries and the capabilities available to them. Dissatisfaction with the current set of international rules, norms, and agreements will cause revisionist actors to make their own – and attempt to enforce them. Meanwhile, the loss of legitimacy or strength by governing authorities will permit other actors to effectively employ coercion and violence in pursuit of power or to further their beliefs.

Furthermore, the *Contexts of Future Conflict* should not be viewed in isolation. The Joint Force will almost certainly operate within and across multiple contexts at any given time. Additionally, it is likely to encounter escalating situations characterized by sudden and rapid transitions between contexts. Thus, as a group, the contexts support the development of integrated operational approaches to specific military problems – particularly as actual adversaries develop and execute strategies that pose challenges across several contexts.

The challenges described within and across the *Contexts of Future Conflict* are not necessarily preferred nor are they inevitable. Through its strategic decisions, the United States will actively, and sometimes inadvertently, influence how trends and conditions unfold – and thus the severity or probability of conflict and war within these contexts. Therefore, the successful application of

[12] Colin Gray, *Another Bloody Century*, (2005), p. 55.
[13] This section of *JOE 2035* was derived from a Joint Staff J-7 study titled *Contexts of Future Conflict: Opportunities and Challenges for the Future Joint Force* (September 2015).

military power will be closely linked to the Joint Force's ability to understand the impact of U.S. engagement in the evolving security environment.

Context 1: Violent Ideological Competition

Ideologies are a set of principles upon which a group legitimizes its claim to power, combined with the goals (societal, religious, economic, security) they purport to pursue.[14] Ideologies become a strategic matter for the nation when specific ideas are paired with violence and coercion against the United States, its allies, partners, and interests. The purposes of conducting war through violent ideological competition are to contest rival ideologies for legitimacy; to contend for the allegiance of certain local populations; to motivate like-minded followers to participate in political action – sometimes, but not always violently; and to construct new cross-border and transnational political arrangements. In 2035, the United States will confront identity networks that are constructed in cyberspace, reach transregionally across national boundaries, and are capable of challenging state authority or the institutional, social and cultural structures that underpin a peaceful, orderly world.

Violent Ideological Competition
Irreconcilable ideas communicated and promoted by identity networks through violence.

Character of Conflict

"The empires of the future are the empires of the mind..."[15]

Within this context, conflict and war are likely to occur as ***identity networks communicate and promote irreconcilable ideas through violence***. Although war always contains an ideological component, the expansion of communities of motivated, like-minded individuals who are willing to resort to violence to further a shared vision or cause will amplify the intensity and transregional scope of violent ideological competition in 2035. Identity networks will become increasingly more capable of reaching out locally, regionally, and globally to express diverse beliefs, including ethnic or social consciousness and religious or social change, all achieved through violence.

Using an array of multimedia capabilities and broad access to the Internet, groups will be able to mobilize, connect, and coordinate over wider, non-contiguous areas. The same global information environment that allows ideas to be shared widely will also permit groups to form, plan, and conduct campaigns of violence more rapidly, over wider geographical areas, and in a more coherent and sustained way than is common today. Furthermore, new means to encrypt communications over both the public Internet and ad-hoc mesh networks will securely connect large numbers of persons predisposed to violence.

Violent ideological competition at the sub-state level will likely involve distributed identity networks avoiding states and selectively mirroring their governance functions, such as engaging in trade and taxation. Some identity networks may not seek to capture the state, but to avoid it – making the environment safe for criminal activity. Flows from illicit activities may fuel insurgent groups or otherwise allow hostile organizations to carve out autonomous zones for uncertain or illegal purposes, as well as build military capabilities that rival or even surpass those of their host states.

[14] Mark Haas, *The Ideological Origins of Great Power Politics*, (2005), p. 5.
[15] Winston Churchill, 1943 Speech at Harvard Commencement.

Nature of Potential Adversaries

The future Joint Force will confront a range of adversaries focused on expressing ideas and beliefs through violence. The most probable competition will continue to be centered on violent identity networks advocating radical interpretations of the Islamic religion focused on the rejection of established governments in the Middle East, opposition to continued U.S. and Western involvement in this region, and the construction of a revolutionary state in the Sunni world. These groups will rely on the political activation of both middle-class professionals and disaffected youth, and are currently exemplified by an array of violent extremist organizations (VEOs) such as Al Qaida or the Islamic State.

The future security environment may also witness the emergence of new ideological appeals to violence. Anarchist, hacker, or environmental groups may embrace violent action in concert with computer network attacks or industrial and economic disruption in support of radical political or social change. Europe, for example, may see the emergence of violent nativist organizations opposed to immigration. To the extent that violent political action is perceived as successful, other religious, cultural, or political groups may follow suit and mimic successful operational and tactical approaches.

This context also has a state level component, as a number of countries such as Russia, China, and Iran will continue to activate, guide, and direct identity networks, including foreign proxies, to further their own national interests as well as to avoid overt military engagement. Many authoritarian regimes also perceive the array of social and political organizations that are part of a free society as destabilizing and threatening. Each fears being overthrown through revolution, both peaceful and violent, and often believes that organizations in the West are engaging in ideological competition that poses a severe threat to the stability of their regimes.

Military Competitive Space

> *"In a post-modern society power [is] being exercised through networks. They could mobilize a mass of connected individuals towards a desired objective, allowing them to surge together and out-flank the controlling devices of a vertical bureaucracy."*[16]

Military competition within this context focuses on the ability of identity networks to use ideas to coherently manipulate the mental processes, emotions, feelings, perceptions, behaviors, and decisions of their intended targets. These ideas will be transmitted and reinforced through a combination of narratives, strategic communication techniques, propaganda, and the tailored application of terrorist strikes, raids, cyber-attacks, and other covert or overt military activities. The purpose of these efforts is to change the behavior of targets, to isolate them from outside support, and to deter the involvement of the United States or application of the Joint Force.[17]

Adversary information operations will focus on evolving their messages, goals, aspirations, and objectives and adapting their narrative strategies to affect a variety of friendly, neutral, and hostile audiences. Information warfare and propaganda efforts will be reinforced by military activities and violent action, and may increasingly focus on individual citizens, decision-makers, or service

[16] John Mackinlay, *The Insurgent Archipelago*, (2009), p. 138.
[17] Antulio Echevarria II, "Wars of Ideas and THE War of Ideas," U.S. Army War College (2008), p. 28-29.

members within the United States itself as adversaries improve their ability to match online personas with physical locations. As a result, the need to develop new narratives and novel depolarization techniques favorable to the United States will become more critical.

New manufacturing capabilities combined with an emerging ability to program inexpensive and widely available computer processors may allow identity networks to rapidly build and field sophisticated weapons that may not require sophisticated users to effectively employ. Greater access to sophisticated weaponry will enable small unit, distributed attacks; raiding over wide areas; the disruption or destruction of forward operating bases and embassies; and the targeting of key infrastructure, cultural monuments, schools, hospitals, places of worship, or military personnel and their families within the United States and living abroad.

Furthermore, instead of one-off affairs, terrorist attacks in the future might become coordinated and sustained campaigns with rapidly shifting methods and targets. The continuing spread of technology will provide greater opportunities for potential adversaries to design, resource, and execute complex attacks and combine many complex attacks into larger, more sustained campaigns. For example, simultaneous multi-city and multi-location operations might involve coordinated small unit assaults, improvised and intelligent explosive device placements, and sniper attacks.

The basic asymmetry at play in this context is that while identity networks have few visible targets or infrastructure to defend, the United States, its allies and partners often have expensive and hard-to-replace infrastructure and culturally or politically important symbols that can be easily attacked. As such, it can be difficult to deter adversaries and bring decisive military power to bear against them. Additionally, these networks may be able to force the United States to dedicate increasingly scarce resources on expensive defensive measures, rather than global power projection capabilities.

Context 2: Threatened U.S. Territory and Sovereignty

The United States consists of 50 states and 14 administered territories, including coastal waters, maritime exclusive economic zones, and airspaces (up to sixty miles) adjacent or contiguous to its territory. Defense of the United States is not just protection of the physical integrity of this territory, but also the protection of U.S. citizens and critical infrastructure.[18] The United States has endured attacks and raids on its territory in the past. Among others, these have included the burning of Washington, D.C. by invading British forces in 1814, the surprise attack on Pearl Harbor in 1941, and the terrorist attacks on New York and Washington in 2001. All underscore the enduring requirement for military capabilities and operational approaches to physically defend U.S. sovereign territory and citizenry against a wide range of foreign military operations. In 2035, the United States will confront an increasing number of state and non-state actors with the will and capabilities to threaten targets within the homeland and U.S. citizens with the ultimate intention to coerce.

Threatened U.S. Territory & Sovereignty
Encroachment, erosion, or disregard of U.S. sovereignty and the freedom of its citizens from coercion.

[18] Joint Publication 3-27, *Homeland Defense,* (29 July 2013), p. I-1.

Character of Conflict

> *"…Defenses cannot achieve perfect safety…Just increasing the attackers' odds of failure may make the difference between a plan attempted or a plan discarded. The enemy also may have to develop more elaborate plans, thereby increasing the danger of exposure or defeat."*[19]

Within this context, conflict and war are likely to occur as adversaries become increasingly capable and willing to ***encroach, erode, or otherwise disregard U.S. sovereignty and the freedom and autonomy of its citizens***. Today, defense of the homeland focuses on placing military capabilities as far forward as possible to reassure allies, providing a layered defense of the United States, monitoring the aerospace and maritime approaches to North America, and establishing credible nuclear deterrence capabilities to dissuade attacks. Furthermore, it also includes support to civil authorities for domestic disaster response operations and potential support to law enforcement to repel VEO attacks within the U.S.

The United States faces a future security environment in which it must maintain the capacity to do these things while also preparing for adversaries that will develop more numerous and varied capabilities to hold U.S. citizens and global commitments at risk. Within this context, the United States must simultaneously protect against an increasing range of foreign threats to its homeland while encouraging the greatest degree of autonomy within the international system where the freedom and autonomy of others are often perceived as an existential threat.

Individual American citizens to include key political, economic, or military figures will be subject to information warfare reinforced by violence, focused on influencing broad public opinion or manipulating their decision calculus. Often, these coercive tactics will be difficult to distinguish from criminality because the same globalized world that empowers the United States also blurs the line between criminal entities and terrorist groups. Opportunities to partner between a wide-range of unlawful organizations will continue to complicate and confuse the distinction between law enforcement and military action within the United States, particularly when these networks cross borders.

Nature of Potential Adversaries

The future Joint Force will confront a range of adversaries attempting to breach U.S. borders. Over the next two decades, there will be a significant evolution in long-range strike weapons capable of ranging the U.S. homeland. Russia will modernize its land, air, and sea-based intercontinental nuclear forces. China's recent industrial and economic growth combined with its desire to once again be a regional hegemon and global power may result in new nuclear doctrine emphasizing first use and a counter force approach, versus its current counter value doctrine and capabilities. Future delivery mechanisms might include hypersonic missiles, long-range cruise missiles, and ballistic missiles with maneuverable warheads, all designed to penetrate U.S. defensive systems.

The purpose of state adversary investments in global strike assets capable of reaching North America is to threaten key targets within the United States during a conflict. Although the risk of

[19] *911 Commission Report*, p. 383

direct assault on the U.S. homeland by traditionally organized, equipped, and commanded military forces operating at the direction of a national political authority is probably far lower than most other threats, it has not gone away. Foreign powers may focus strikes or raids on targets which result in larger systemic effects against U.S. economic or power projection capabilities.

Some sub- or transnational groups see the United States as underwriting world order and believe that delivering catastrophic damage to the U.S. homeland will serve to divert U.S. military power from interdicting them overseas. VEO and irregular/special operations forces (SOF) networks are likely to have the capacity to organize, train, and equip within the U.S. itself. These non-state actors may launch attacks within the homeland to prevent the United States from interfering with their goals and objectives. Although this strategy has historically failed, its frequent appearance suggests that weaker adversaries still believe they can deliver a blow against the homeland that may keep the United States from engaging.

Military Competitive Space

> *"…we can expect that future attacks will aim at both large-scale casualties and symbolic targets…[they seek] high body counts, go after iconic targets, and cause economic damage. The terrorists will continue to demonstrate tactical adaptability, which will make it difficult to plan security measures around past threats or a few threat scenarios. Terrorists innovate."*[20]

Military competition within this context will revolve around the ability of adversaries to influence, deter, and coerce the United States through the credible threat of violence against its homeland and citizens. The frequency and array of adversary deterrent operations are likely to increase, to include snap nuclear exercises, bomber flights, and strategic reconnaissance overflights into U.S. ADIZs as typically conducted by Russia. China may conduct similar global deterrent operations through maritime presence operations near U.S. territories and bases throughout the Pacific. From time to time, even smaller regional powers such as Iran and North Korea may attempt deterrent missions.

The Joint Force will need an array of capabilities to complicate or defeat the deterrent strategies of adversaries. These will include aerospace awareness sensors and layered antiballistic missile systems, but also maritime capabilities to counter patrols by adversary submarines and long-range unmanned submersibles used against underwater infrastructure in U.S. territorial waters and Exclusive Economic Zones. Creating these capabilities will naturally increase the incentives for the United States to divert already scarce defense resources away from its own global power projection capabilities to focus more on homeland defense measures.

Adversaries may also attempt to disrupt the ability of the United States to conduct overseas military operations through attacks on major nodes of the global trade and logistics network such as large container ports or major airports. Some adversaries might also attempt to attack military bases and facilities to disproportionately degrade the ability of the United States to generate, deploy, and maintain the Joint Force. The development of small, smart, cheap, autonomous, long-range, and highly-capable systems operating in the air, land, sea, and undersea environments may further

[20] RAND Corporation, *The Lessons of Mumbai*, (2009), p. 21

complicate the homeland defense mission by providing relatively cheap strategic attack options to both state and non-state actors.

In the future, the Joint Force may confront heavily-armed violent extremists operating in the homeland armed with small drones and weapons delivery devices built with off-the-shelf components, using additive, three-dimensional, and other sophisticated manufacturing techniques. This may allow terrorist and state-sponsored Special Forces to self-generate capable units within the United States. These forces might be able to create small-unit overmatch against local police, and perhaps, sustain small-scale but violent attacks, to include the use of smart IEDs or novel biological and chemical weapons.

The basic asymmetry at play is that adversaries will be able to credibly threaten to strike the United States and increase the costs of foreign engagement. Adversaries will threaten the homeland not to physically destroy the United States, or even in anticipation of materially hindering its economic or military potential, but rather to change the decision calculus of leaders or the public's appetite for foreign military operations. At times, these operations may be purposely ambiguous in nature to intentionally complicate the Joint Force's ability to quickly and effectively respond.

Context 3: Antagonistic Geopolitical Balancing

No state has succeeded in completely replacing the international system with a globe-spanning empire, and even a large and powerful state like the United States cannot entirely control or dictate the course of global affairs. Historically, powerful states have always encountered resistance to their strategic objectives and attempts to restrict their freedom of action. This resistance may include the fielding of deterrent military capabilities or the development of alternative military alliances and partnerships. It may also take the form of offsetting technological initiatives, increased industrial development, ideological subversion, unconventional warfare, or other propaganda activities. The United States will be challenged to protect allies and interests around the world while simultaneously avoiding security dilemmas and managing potential escalation to open conflict with other competitor states. In 2035, the United States could find itself confronted by several states with diverging, conflicting, or opposing interests who may form active coalitions that present coordinated resistance to U.S. influence, presence, and power projection around the world.

Antagonistic Geopolitical Balancing
Increasingly ambitious adversaries maximizing their own influence while actively limiting U.S. influence

Character of Conflict

> *"If the three land masses of the Old World can be brought under the control of a few states and so organized that large unbalanced forces are available for pressure across the ocean fronts, the Americas will be politically and strategically encircled"*[21]

Within this context, conflict and war are likely to occur as ***powerful and increasingly ambitious adversaries actively work to maximize their own influence while excluding or limiting U.S. influence***. Until quite recently, the application of active balancing activities against the United States was limited in scope and scale. The relative power of the United States immediately

[21] Nicholas Spykman, *America's Strategy in World Politics* (1942). p. 448.

following the collapse of the Soviet Union, a growing economy, a system of alliances coupled with a formidable global basing network, and the very visible display of U.S. military power in the first Gulf War induced a significant amount of caution in competitors wishing to challenge the United States, its allies, partners, interests, and overall global position.

Over the next two decades, the United States will likely maintain its position as the single most powerful actor on the world stage. However, while no power or coalition of powers has yet emerged to openly oppose U.S. global influence and reach, the United States will operate in a world in which its overall economic and military power, and that of its allies and partners, may not grow as quickly as potential competitors. The rise of economic near-peer competitors outside of the U.S. alliance system is critically important because "economic might is the foundation of military power…and a reliable way to gain a military advantage over rivals."[22]

As some states fully emerge as leading actors in the globalized economy, they are likely to gain a new sense of power and confidence with each scientific, economic, and social achievement. Inevitably, this success will encourage them to advocate their own ideas about how economic and strategic relations with other states should be governed. The United States will encounter powerful states reaching for regional supremacy, rearranging borders, and constructing new economic and political arrangements. They will attempt to hinder the ability of the United States and its allies to work together and actively try to isolate key alliance members. Further, they might encourage or coerce them to leave the alliance structure altogether.

Nature of Potential Adversaries

For the foreseeable future, the rising economic and cultural power of some Asian countries, particularly China, is breeding new and more expansive political and geostrategic ambitions backed by growing military power. In other areas, the historical logic of imperialism, sometimes accelerated by economic and demographic decline, is leading to reactive aggression designed to blunt or erode U.S. influence regionally. Examples include Russia's renewed political/military aggression in Europe, the Caucuses, and Central Asia; Iran's cultural/religious bid for hegemony in the Middle East; and North Korea's ongoing efforts to detach U.S. political and military support to the Republic of Korea.

Revisionist states will be increasingly dissatisfied with the current Western-derived notion of international order. For example, Vladimir Putin noted that in the Russian view, uncontested Western leadership means an international environment in which "no one feel(s) safe, because no one can feel that international law is like a stone wall that can protect them."[23] In these cases, states may use military power to establish (or reestablish) local spheres of influence, create buffer states or regions which are subordinate and/or dependent on the local hegemon, and disconnect neighboring states from the broader global economic and political system.

Major state competitors will try to weaken traditional U.S. alliances or take advantage of perceived fractures to expand their regional power. Although seemingly insignificant today, organizations such as the Shanghai Cooperation Organization and the Eurasian Economic Union could grow as

[22] John Mearsheimer, *The Tragedy of Great Power Politics* (2014) p. 142.

[23] Vladimir Putin, as quoted in Robert Kagan, "The End of the End of History: Why the 21st Century will look like the Nineteenth," *The New Republic*, (April 23 2008).

China, Russia, India, and others turn to these multinational groups to reorder international rules in their favor. Russia, China, and other revisionist states may also increasingly partner and coordinate with each other or with smaller, but militarily-active partners such as Pakistan or North Korea. Russia is likely to extend its influence and control in Eastern Europe and Central Asia by presenting itself as the security partner of choice. In Asia, China might attempt to weaken alliances and compel neighboring states to recognize its hegemony in the region.

Military Competitive Space

> *"We have to recognize that there are two authoritarian nuclear-armed regimes dominating the Eurasian landmass, and they are using or threatening to use a broad spectrum of force against their neighbors."*[24]

The military competitive space here will primarily be marked by encounters in a "zone between war and peace [and] the United States must be able to conduct many different types of missions within that zone."[25] Competitor states are likely to employ hybrid stratagems using a confusing combination of direct and indirect approaches to contest U.S. global interests. These approaches will be designed to avoid overt commitment to major foreign operations, minimize the risk of escalation, provide plausible deniability, and avoid the costs of direct involvement. They may be characterized by credible threats to take and hold key terrain near their borders, an intensification of warfare by proxy, and the employment of new technologically-advanced military capabilities. Further, these conflicts will feature regional nuclear deterrence in support of conventional military operations and a desire to build 'off ramps' to avoid escalation with the United States.

Several state adversaries will be able to threaten and quickly take key territory or terrain near their borders, using conventional, mechanized combined arms forces, spearheaded by Special Forces and even local proxy insurgent groups. Once in control of an objective, these states will then deploy sophisticated and layered air defenses, advanced manned and unmanned aircraft, long-range ballistic and cruise missiles, submarines, surface ships, electromagnetic jammers and spoofers, and cyber techniques to hold and protect these territories while simultaneously keeping the United States and its allies at a distance.

Complementing the ability to seize and hold key terrain, some strike assets will be physically located within an adversary's homeland, raising the possibility of escalation to nuclear conflict if attacked by U.S. or allied forces. This consolidation of regional hegemony on land will then give some states the strategic depth to invest in the naval, air, cyber, and other capabilities necessary to build credible power projection capabilities and assert themselves farther from their borders. While large-scale, open economic warfare between major states is unlikely, some states might use more limited, and covert tactics, such as sanctions, blockades, sabotage, and corporate espionage against local targets, all protected under an umbrella of long-range strike capabilities.

Furthermore, the United States will likely see a number of states that can generate military advantages locally in ways that match or even exceed that of the Joint Force and its partners. U.S. superiority in high-tech warfare will be met by asymmetric, unconventional, and hybrid responses

[24] Lt. Gen. James Kowalski, Deputy Chief Strategic Command (16 June 2015).
[25] Spencer Bakich, "Can Cooler Heads Prevail in the U.S./China Military Relations?" *The Bridge* (19 June 2015).

from adversaries, as opposed to countering the United States on a technology-by-technology and platform-by-platform basis. "Moreover, rapid globalization and diffusion of technology has lowered the barriers for [even] smaller states…to acquire and field advanced military capabilities or inexpensive but highly effective asymmetric capabilities such as robotic swarms." [26] Accelerating efforts by adversaries to apply a variety of new technologies will threaten to frustrate the Joint Force's ability to close from strategic and operational distances.

The future Joint Force will be challenged to break the power projection capabilities of adversary states, including modern mechanized forces on land and sophisticated naval forces at sea, all protected by advanced aerospace and electromagnetic jamming and spoofing capabilities. Furthermore, a number of adversaries will invest in hypersonic weapons, and the first nation to successfully deploy an operational system will gain significant military advantages due to the speed at which targets can be engaged. Functional hypersonic systems will ultimately provide a regional strike capability which might potentially disrupt Joint Force power projection.

Context 4: Disrupted Global Commons

Prosperity of the United States depends upon its largely uncontested ability to access and use the global commons, which consist of those areas that "belong to no one state and that provide access to much of the globe."[27] The commons includes spaces at sea and in the air outside of a state's territorial waters (generally defined as 12 miles from a coastal baseline), and outer space (particularly in orbit from 60 to 22,300 miles above the surface of the Earth). Additionally, the electromagnetic spectrum – particularly access to signals for communications, position, navigation, and timing – must be considered part of the commons.[28] Open and accessible global commons are the pillars of the current international economy and empower states that use them to conduct commerce, transit, scientific study, or military surveillance and presence. In 2035, the United States will find itself challenged in parts of the global commons as states and some non-state actors assert their own rules and norms within them.[29]

Disrupted Global Commons
Denial or compulsion in spaces and places available to all but owned by none.

Character of Conflict

> *"Since men live upon the land and not upon the sea, great issues between nations at war have always been decided—except in the rarest cases—either by what your army can do against your enemy's territory and national life, or else by the fear of what the fleet makes it possible for your army to do."*[30]

---

[26] Shawn Brimley, Ben FitzGerald and Kelly Sayler, "Game Changers: Disruptive Technology and U.S. Defense Strategy" *Center for a New American Security Disruptive Defense Paper* (September 2013).

[27] Barry Posen, "Command of the Commons: The Military Foundation of U.S. Hegemony," *International Security*, Vol. 28, No. 1 (Summer 2003), Posen attributes the origin of the term to Alfred Thayer Mahan, who described the sea as "a wide common, over which men may pass in all directions." *The Influence of Sea Power upon History: 1660-1783*. (Boston: Little, Brown and Co., 1890), p. 25, while the According to the United Nations Environment Program (UNEP), global commons are "domains that lie outside the political reach of any one nation state."

[28] This context deliberately excludes cyberspace, which is described in detail in ***Context 5: A Contest for Cyberspace,*** on page 36.

[29] Scott Jasper (ed.) *Conflict and Cooperation in the Global Commons* (2012). p.2.

[30] Julian Corbett, *Some Principles of Maritime Strategy*. (1918), p. 12.

Within this context, conflict and war will likely revolve around the ***denial of or compulsion within spaces and places available to all but owned by none.*** The international norm of free and open global commons is principally underwritten by the political influence and military power of the United States. Since the end of World War II, the United States assumed chief responsibility for protecting the commons, establishing shared rules and norms for their use, and encouraging wide recognition and support for these rules and norms by other states. The United States relies on unrestricted use of the global commons to connect with its allies and partners and support its interests and commitments around the world. Therefore, the United States dedicates considerable effort and military resources to ensure the global commons remain open, stable, and protected.

This context describes a future environment in which access and use of the global commons cannot be taken for granted. As states become more capable of operating within the commons, they are likely to develop – and attempt to enforce – their own rules and norms for acceptable use of the commons. This might include new interpretations of freedom of navigation at sea or the assertion of new economic rights in disputed continental shelf zones. They may also institute restrictions in aerial approaches to their homeland or try to deny the operation and use of satellites in orbit. Some states might also selectively regulate, jam, or otherwise deny electromagnetic frequencies in ways that may be incompatible with U.S. strategic interests.

The commons in 2035 will be more congested, contested, and competitive. [31] Although the United States is not likely to lose access to the commons as a whole, it will encounter an increasing number of states able to threaten or restrict its freedom of action in the commons. Successful efforts to disrupt or deny use of the seas, air, space, and the electromagnetic spectrum will degrade the ability of the United States to connect with the global economy, support allies, and link military forces together over wide areas. Denial of the commons, taken to its logical conclusion, could allow adversaries to isolate the United States from friends and allies around the world. Control of the commons by adversaries would then allow them to eventually project power from the commons into the United States itself.

Nature of Potential Adversaries

The United States can expect some states to begin enforcing their own interpretations of acceptable behavior in the air and maritime commons. Over the next two decades, an increasing number of states will enhance their ability to monitor and patrol the air and sea farther offshore. This will include a range of surveillance and patrol activities in strategic locations such as the East and South China Seas and the Indian Ocean, and near strategic maritime choke points to include the Straits of Hormuz, Malacca, Sudra, and Lombok, and the Red, Yellow, and Okhotsk Seas. There will be an elevated risk of many different forces colliding or otherwise interfering with one another in these areas, potentially disrupting international commerce.

The United States will also be increasingly encumbered by regulatory restrictions in maritime zones within 12 to 200 nautical miles of coastlines. Some states will attempt to extend administrative control over commercial activities transiting their continental shelf areas and EEZs. They will use new legal constructs to hinder or obstruct the innocent passage of reconnaissance and military patrols by other states, outside of generally recognized 12 mile territorial limits. These

[31] *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (2012), p.2.

will be backed by increasingly capable and numerous adversary maritime assets, including patrol aircraft, coast guard vessels, and advanced undersea warfare capabilities.

The maritime, air, and space commons are connected by the electromagnetic (EM) spectrum. Signals at various frequencies in the EM spectrum are used for a number of purposes, including radar imaging sensors, cell phone networks, Wi-Fi signals, simple AM or FM transmissions, and position, navigation, and timing signals.[32] Although traditionally governed by national rules within national territory, conflicting views between states about assured use of important parts of the electromagnetic spectrum, particularly during crisis and war, is likely to lead to active competition. Adversaries will attempt to maintain their use of the EM spectrum while denying it to others.

Military Competitive Space

> *"Of particular concern [is] the proliferation of…technologies designed to counter U.S. military advantages* ***and curtail access to the global commons.****"*[33]

By 2035, command of the commons will translate into significant military advantages, and the ability to operate in and through all of the commons will be central to the design of military forces. The cumulative effect of broader adversary reach into the commons may be to increasingly slow, hinder, and erode their use by the United States for economic and political purposes. In the future, parts of today's free and open commons may be disrupted by a combination of active opposition to existing norms, the maturation of anti-access and area denial capabilities, and the development of new power projection capabilities to control and manage these spaces.

The implications of increasing adversary abilities to both see and reach into the commons will be particularly acute in the air and sea spaces near their borders. The Joint Force can expect competitors to increasingly challenge U.S. presence. Many states are expected to develop highly capable ISR assets, including UAVs and advanced radars, to find and track U.S. forces. The application of offensive electronic warfare will be used to jam, spoof, blind, or dazzle U.S. platforms. Additionally, use of the air domain may be increasingly contested by high power laser and microwave weapons, which are especially effective against fragile airframes, sensors, and electronic components. Some states might also position advanced air and missile defense systems in protected locations, such as homeland territories or indigenous islets, to deny freedom of movement to the Joint Force.

The space commons is the primary medium of military communication, data transmission and ISR. Although the United States currently possesses a pronounced advantage in space-based sensors, Russia, China, and other nations have developed increasingly capable space-based C3/ISR systems. Competition in orbit (even during peacetime) will be intense, highlighted by satellites maneuvering to hinder the operations of other satellites, co-orbital jamming, and the use of ground-based lasers to dazzle or destroy imaging sensors. Future adversaries will also have the capability

[32] The electromagnetic spectrum describes the full range of range of radiation frequencies delivered via photons, and spans radio waves, microwaves, millimeter waves, infrared (IR) radiation, visible light, ultraviolet radiation, x-rays, and gamma rays. It is a physical phenomenon defined by the frequency, power, and time of the radiation in question. Joint Concept for Electromagnetic Spectrum Operations (18 March 2015), p. v.
[33] National Military Strategy of the United States of America (2015).

to deploy blockers and grapplers to impede the free operation of commercial and military satellites, and they will use ASAT weapons launched at space assets from the ground as well as from other satellites. Ultimately, this may generate space debris leading to a runaway chain reaction which destroys other satellites and threatens the integrity of many important orbits.

The near-uncontested freedom to operate on the seas, through the air, in orbit and over the electromagnetic spectrum has provided the United States with a high degree of freedom of maneuver and the ability to securely trade with partners around the world. It has also when necessary allowed the Joint Force to project power and concentrate force in order to effectively conduct military activities on other continents. However, it is very unlikely that future adversaries will allow U.S forces to move through the commons to forward positions and await a set-piece U.S. onslaught as, for example, the Serbs or Iraqis did in the past. The next two decades will see adversaries building the capacity to control approaches to their homelands through the commons, and later, translating command of the nearby commons into the connective architecture for their own power projection capabilities.

Use of the commons is central to influencing events abroad, and as the sea, air, space, and electromagnetic capabilities of others grow, competitors will increasingly use the commons for their own military purposes. In the future, the Joint Force will encounter "combined swarms" featuring seabed, subsurface, surface, and aerial unmanned, autonomous platforms. These will be used to observe more of the commons at high resolution and complicate defensive efforts. Conflicts in the commons will feature repeated attempts by adversaries to mutually disrupt one another's power projection capabilities – often from great distances, and to develop and safely use bases at home and within the commons themselves to influence events on land.

Context 5: A Contest for Cyberspace

The United States depends on an interdependent network of information technology that includes the Internet, telecommunications networks, computer systems, embedded processors and controllers – and the data, information, and knowledge that is stored in and flows through these systems – for its economic, industrial, societal, and military well-being. This domain – cyberspace – has emerged as a significant setting within which strategic competition takes place. The United States will continue to be involved in a global struggle to define and defend this domain. State actors will attempt to make clear distinctions between sovereign and non-sovereign parts of cyberspace, while cyber-capable non-state actors, hacktivists, and other individuals might take action to complicate or ignore these distinctions altogether. In 2035, the United States will need to defend its sovereign cyberspace, protect the use of non-sovereign cyber commons, and control key parts of cyberspace (both sovereign and non-sovereign).

A Contest for Cyberspace
A struggle to define and credibly protect sovereignty in cyberspace.

Character of Conflict

> *"…because cyberweapons are not overtly violent, their use is unlikely to fit the traditional criterion of interstate war; rather, the new capability is expanding the range of possible*

harm and outcomes between the concepts of war and peace—with important consequences for national and international security…"[34]

Within this context, conflict and war are likely to occur as states ***struggle to define and credibly protect sovereignty in cyberspace.*** Defining the boundaries that exist between sovereign and non-sovereign areas has always been difficult, contentious, and usually resolved through war. In each of the terrestrial domains (land, sea, and air), the delineation of boundaries, rights, and responsibilities took time to fully establish, was (and continues to be) contested, and eventually required the creation of basic and mutually acceptable rules and norms governing their use. The Treaty of Westphalia, which defined the modern notion of the nation-state and "national sovereignty," was explicitly designed to lower the risk of violence and war. Ultimately, it took violence out of the hands of individuals, privateers, militias, and mercenaries, and imposed reciprocal responsibilities on states to recognize one another's borders and internal autonomy.

Rules and norms are poorly established in cyberspace. Thus, the same dynamic of states defining and defending sovereignty in cyberspace is likely to play out over the next several decades Although frequently referred to as part of the global commons, few Americans believe that government and DoD systems, corporate networks, or personal banking and financial accounts are "owned by none, accessible to all" according to the classic definition of what constitutes a commons.[35] The reflex to think of cyberspace as a commons is perhaps reflective of the design philosophy underpinning the Internet which is based on shared standards, an open exchange of information, and accessibility.

Today, the cyber domain is so integral to the basic infrastructure of the United States and the larger global economy that actions to deny, degrade, or destroy parts of it have the potential to create intolerable security problems. The contest in cyberspace will continue to be fraught with misperception and miscommunication, particularly with regard to the proportionality of damage caused by cyber-attacks and equivalent consequences in the other domains. By 2035, international norms might be created and adopted that define what is sovereign versus what is common in cyberspace. As a result, a range of cyber activities will be increasingly and more comprehensively linked with national security strategies.

Nature of Potential Adversaries

The United States and other states will certainly wish to survive and thrive in cyberspace. However, in an environment where the difference between national and "common" cyberspace is ill-defined, there will be a greater degree of ambiguity, friction, conflict, and war with a wide range of cyber-capable actors. Not all states will take the same approach to cyberspace control. However, many competitor states, reacting to the growth of the information-rich and uncontrolled global Internet, will continue to develop cyber-security organizations and install barriers such as China's "Great Firewall" to protect their critical cyber infrastructure, monitor domestic opponents, and control the flow of information within their borders.

In many places, the next few decades will see the development of cyberspace with more authoritarian characteristics focused on limiting access, connections, and compatibility with the

[34] Lucas Kello, "The Meaning of the Cyber Revolution," *International Security*, (2012).
[35] See "Context 4: Disrupted Global Commons" above.

rest of the world. For example, a new draft Chinese cyber law "is formulated…*to preserve cyberspace sovereignty, national security and societal public interest.*"[36] Here, military cyber forces will assist national authorities to delineate and defend "national" borders in cyberspace, and to construct and enforce the protocols and rules governing its operation and use at home. Ultimately, the more active control of cyberspace by authoritarian powers may provide them a distinct military advantage.

The cyber forces and activities of many states will also likely be used to stress or fracture the social and political cohesion of competitors. Some adversaries will develop cyber strategies and information-related capabilities designed to influence the perceptions and decision calculations of their opponents. Proficiency in cyber operations will provide states a rather precise set of capabilities to potentially affect the attitudes, behaviors, and capabilities of other states at great distance, persistently, and relatively cheaply. Furthermore, cyber activities by foreign states and hacker groups are likely to be extremely personal as adversaries attempt to influence key U.S. political, business, and military leaders through targeted information warfare.

Military Competitive Space

> *"Cyber power projection…refers to the capability of a government to intimidate other nations and implement policy by means of force from cyber actions or the threat thereof."*[37]

The intersection of cyberspace and sovereignty will lead to new modes of conflict. Dependence on a range of capabilities in this domain coupled with the vulnerability of cyber-enabled systems to exploitation presents an assailable flank which competitors are likely to probe, infiltrate, and potentially attack. This contest for cyberspace will involve any digital, code-enabled system that can communicate, emit, connect, or sense. States will likely use cyber operations to safeguard their own critical national infrastructure while simultaneously attempting to influence, disrupt, degrade, or perhaps even destroy that of their competitors.

A growing number of states will have extensive offensive cyber forces at their disposal to disrupt the smooth and efficient functioning of cyber-connected systems. In the future, state military and security organizations will increasingly use cross-border network and web-site disruptions to cause social unrest. Attacks will work to undermine the trust and data integrity that are central to advanced societies, particularly financial, legal, and technical infrastructure. This competition may also feature strategic surveillance as well as industrial and scientific espionage. Additionally, the competition may involve disrupting data, networks, and the physical systems of competitors to gain economic, military, and political advantages.

Adversaries may also attempt to conduct a strategic cyber campaign directly against the U.S. homeland focused on degrading critical systems and assets. The Joint Force will likely have a role

[36] Draft Cybersecurity Law (China). This law asserts the need to maintain cyberspace sovereignty through national measures such as real name registration for domestic cyberspace users, "support and assistance" to the government for dealing with criminal investigations, review of cybersecurity practices of key telecommunication operators by the Cyberspace Administration of China (CAC), and the collection and storage of user data within China.
See also, Council on Foreign Relations: http://blogs.cfr.org/cyber/2015/07/08/chinas-new-cybersecurity-law/.
[37] Kevin Coleman, "Aggression in Cyberspace," in Jasper (Ed.) *Conflict and Cooperation in the Global Commons*, p. 110.

in protecting the integrity of critical networks, cable transports, servers, the software that supports financial systems, and national-security related information as it would other sovereign parts of the United States. This competition will likely feature the increased ability to damage important industrial machinery, and to inflict physical damage – both widely or precise as necessary – through connected and compromised robotic and autonomous systems.

Some states may also integrate cyber warfare capabilities at the operational and tactical levels of war, attempting to degrade military networks in order to adversely affect the Joint Force as it deploys or operates in the field. Cyberspace adds a new dimension to the future security environment, allowing military operations to reach across the globe and down to the individual desktop, server, router, or controller chipset level. Where land and naval power intersect in two dimensions, air and space in three, cyberspace intersects with other domains in thousands, or even millions of ways. This presents many new vulnerable points through which weapons systems, and the circuitry and software upon which they rely, will be directly engaged.

In the future, the physical structure of cyberspace will be extremely vulnerable to attack by an array of destructive weapons, including high-power microwave munitions and laser systems which are increasingly effective against digitized, miniaturized, and integrated circuits. Additionally, hypersonic weapons and robotic swarms will increase the tempo of conflict and will be countered by the development of artificial intelligence for battlespace characterization and management. The Joint Force will be required to consider the nature of these advanced artificial systems and how to both defeat and protect systems that reside within the cyber domain.

Context 6: Shattered and Reordered Regions

The inability of states in certain areas of the world to provide stable and legitimate governance will continue to be a significant cause of conflict and war in the future. Stressed by the pace of economic and geopolitical change and not possessing sufficient margins to absorb or adapt to future shocks, weak states might be unable or unwilling to take advantage of commercial opportunities within the global economy. A lack of education and infrastructure might preclude participation in some cases while authoritarian governments might also purposely attempt to isolate its people from external influence. Furthermore, local populations will, through social media, be able to readily the contrast the failure of their governments with economic growth and opportunity in other parts of the world. In 2035, the United States will confront a steady decline in the legitimacy of state authorities unable to adequately govern in many parts of the world.

Shattered and Reordered Regions
States unable to cope with internal political fractures, environmental stressors, or deliberate external interference.

Character of Conflict

> *"…a number of states have erupted into mass violence stemming from internal conflict. Some of these crises are ethnic conflicts. Some are civil wars. Others take on the form of revolutions. Many result in complex humanitarian emergencies. Though the dynamics may differ in each case, all of these conflicts stem from social, economic, and political pressures that have not been managed by professional, legitimate, and representative state institutions."*[38]

[38] U.S. Fund for Peace, *Fragile States Index*, (2015).

Within this context, conflict and war are likely to occur as ***states are unable to cope with internal political fractures, environmental stressors, or deliberate external interference***. As governments fail to provide a regular legal framework, to develop economic stability, to adequately respond to man-made and natural disasters, and to protect their citizens, they will become susceptible to violent political action. Ultimately, multiple internal pressures might eventually cause a state to shatter, a condition where the central government is no longer capable of providing effective and legitimate governance, creating security threats that might affect neighbors and spread regionally.

Weak and fragile states might become the target of more capable external powers that will increasingly exploit internal political, ethnic, or economic fractures to further their own strategic interests. States under stress may also shatter due to these external pressures. Additionally, these states once shattered, may then be forcibly partitioned, subdued, or reconnected by more powerful states, or even very capable non-state or transnational actors. Moreover, damage resulting from the chaos of shattered and reordered regions is not limited to the areas ostensibly under the control of the weak state, but will have consequences for the wider international system.

Conflict in this context will have a significant urban dimension. The lack of connections between new urban migrants and established social structures can potentially lead to friction among sectarian or ethnic groups, and potentially result in the sectioning of cities by religious or ethnic affiliation. Alienation of populations within these areas caused by both poverty and the disorientation of formerly rural residents interacting with more cosmopolitan urban citizens may increase the potential for criminal and gang-related activities as well as the development of urban insurgent groups. Furthermore, the economic, social, and political unravelling of a city, particularly a megacity, would overwhelm the capacity of most states and global humanitarian response communities to effectively respond.

Nature of Potential Adversaries

Ineffective governance in weak states can ultimately lead to the emergence of sub-state actors who oppose or seek to overthrow ruling authorities. While some groups will have legitimate grievances against the state, others will exploit weakness by the central government as justification to seize power, resources, or strategic territory. Increasingly, national borders may be challenged as unresponsive to local political aspirations. Consequently, as internal authority is challenged and begins to collapse, violence is likely to occur in the form of sectarian strife, ethnic conflict, or even civil war.

Shattered states are often safe havens for criminal and extremist organizations, providing their own type of order, however violent or illegitimate. Criminal networks in these environments serve as critical hubs to global black markets that traffic in drugs, weapons, and people. Furthermore, criminal activity within these shattered zones can become the de facto economy of extremist organizations operating in the region. Left unchallenged, these criminal networks might become capable enough to challenge the sovereignty of even functioning states.

Shattered regions can also lead to the emergence of violent groups that sustain themselves by disrupting resource and trade routes, which can cause large-scale damage or negative long-term geopolitical consequences. For example, shattered sovereignty in Somalia allowed for poaching by international fishing companies and the subsequent decimation of the Somali fishing industry.

This in turn led to the creation of local Somali militias to protect their fisheries. These groups then transformed to conduct piracy against international shipping off the Horn of Africa. Eventually, these disruptions encouraged even more consequential and far reaching effects, including accelerating the re-emergence of global Chinese naval power.

Military Competitive Space

> *"More and more of what goes on in other countries matters for the health and safety of the United States and the rest of the world. Many of the new dangers—such as health pandemics and transnational terrorist violence—stem from the weakness of states rather than their strength."*[39]

A wide range of insurgents, transnational extremists, and other states are likely to exploit failures by central governments. This environment will include a shifting array of alliances, partnerships, and relationships featuring, among others, transnational terrorist organizations, global cyber activist networks, private military firms, mercenary groups, and super-empowered individuals. New forms of "shadow" governance will likely emerge where organizations the United States deems illegal or illegitimate begin to fulfill citizens' needs, and problematically, are seen as legitimate by the local population.

Urban centers may become sources of power for insurgent groups by linking them to the wider global black market economy, as they seek to seize control and provide quasi-governance. Ungoverned urban zones are likely to permit the development of new or expanded black markets, including illicit flows of goods, drugs, weapons, currency, and human trafficking. As distinctions between terrorist financial operations and criminal activities continue to blur, the transactional connections between unlawful organizations are likely to confuse the distinction between law enforcement and military action. Additionally, the potential exists for better-resourced terrorist groups to operate more freely across geographic boundaries and exploit jurisdictional gray areas.

Competitor states will exploit weak sovereignty in neighboring states to assert the preeminence of their own national interests and potentially incorporate shattered regions into their own spheres of influence. These assertive states will attempt to reconnect fragile and failing states to their economic and political systems and employ a variety of means to interfere in the internal affairs of those states. They will do so by exploiting the information environment, creating pretexts for action through propaganda, political subversion, and the targeted coercion of leadership.

In some cases, open intervention, including the outright invasion of a sovereign neighbor nation might occur and lead to large-scale, state-on-state conflict. However, there is a greater likelihood that stronger states will expand their use of covert and irregular tactics against weaker neighbors in an effort to internally fracture them. For example, recently fractured states around the Russian periphery present a number of levers that Russia may use to expand its influence and reorient economic and political interests. Strong external powers may also seek to fracture weak states as a way to undermine U.S. regional interests or distract the United States from other more important or consequential priorities.

[39] John Ikenberry, "A World of Our Making," *Democracy*, (Summer 2011).

The Joint Force must be prepared to assist in developing the capacity of partner nations that are most likely to be threatened by external states so that U.S. forces do not have to respond to every crisis. If and when conflict eventually occurs between a partner nation and external threat, the United States is not likely to initially deploy a large ground force. In these situations, the Joint Force will be called upon to bolster the government of a failing state by working with and through host nation security forces to contain and eventually defeat insurgent or separatist movements. Facilitating the local capacity to legitimately govern and be resilient in the face of external and internal shocks will require long-term, clearly understood commitments.

Summary

This section described six individual *Contexts of Future Conflict*. Each context illustrates a particular aspect of conflict in 2035, the nature of potential adversaries, and the likely military competitive space. Looking across the contexts strongly suggests the United States will engage in multiple, simultaneous, and usually trans-regional conflicts involving a broad range of actors. Many adversaries will selectively contest and support international rules and norms while also encouraging or disrupting social, economic and political order based on the scope of their strategic interests and cultural perspectives. Moreover these adversaries are likely to field advanced weaponry leading to potentially increased deterrent, coercive, and warfighting effect.

Together, these large and globally connected problem sets featuring more capable adversaries will place difficult demands on the United States. The Joint Force will be challenged to both protect the global order as currently configured and to resist or discourage the spread and intensification of political and social disorder around the globe. Furthermore, protection of open and broadly favorable international norms and support for a stable political order will be highly dependent on popular perceptions, attitudes, and broad acceptance of their legitimacy. Across all contexts, the ability to engage with ideas and to link the application of physical military power to international legitimacy and good governance will determine the effectiveness and sustainability of Joint Force operations.

Individual contexts are not sufficient to fully understand the missions the Joint Force will need to conduct in the future. For this reason, the next section of *JOE 2035* describes the full range of likely missions by linking each context to four enduring U.S. strategic goals and four associated high-level military tasks. The intersection of each *Context of Future Conflict* with the pairing of strategic goal and supporting military task results in a discrete mission that describes what the Joint Force may need to do given a specific situation. In reality, the future will not present itself in such an orderly way. Conflict will remain, as in Clausewitz's time, "uncertain, variable, and intertwined," and attributes of more than one context may be in play at any given time. However, as a set, the linkage of contexts to strategic goals and military tasks provides a comprehensive view of the range of Joint Force missions and how they are likely to evolve through 2035.

Section 3 - Implications for the Joint Force

> "*Political leaders think in terms of policies and options. Geopolitics teaches us to think in terms of constraints and limits."*[40]

The United States will face a wide range of emerging – and often unforeseen – challenges in the future security environment featuring both *contested norms* and *persistent disorder*. Specific U.S. strategic and military objectives to address these challenges will be many, multi-faceted, and tailored to a specific time, place, and set of circumstances. However, the JOE relies on a range of strategic goals to describe the overall terms of national commitment and articulate an acceptable end state for any particular U.S. strategic endeavor. These are:

1. ***Adapt to changing conditions*** – ensure the United States can adequately cope with emerging changes in the security environment.
2. ***Manage antagonism and impose costs*** – discourage changes to the security environment that are unfavorable to the United States.
3. ***Punish aggression and rollback gains*** – block and undo changes to the security environment that are dangerous or disruptive to the United States.
4. ***Impose change and enforce outcomes*** – introduce desired changes to the security environment that are favorable to the United States.

This range of strategic goals suggests differing levels of engagement, commitment, or overall posture by the United States. Moreover, this range of goals represents a continuum and may change over time as a particular situation evolves. At the low end of this continuum, the United States might reactively manage security threats or otherwise respond to the consequences of natural and humanitarian disasters. At the high end, the United States might proactively solve a security problem by imposing a U.S. preferred solution that forces an adversary to accede to its will.

The role of the Joint Force is to apply military power to support the achievement of strategic goals in concert with other elements of national power. To effectively pursue this range of goals, the Joint Force conducts four types of enduring military tasks against an array of competitors and in response to a range of phenomena. These are:

1. *Shape* or *contain* to assist the United States with coping and adapting to changed international security conditions.
2. *Deter* or *deny* to manage the antagonistic behavior of competitors or to impose costs on competitors or adversaries taking aggressive action.
3. *Disrupt* or *degrade* to punish aggressive action by an adversary or to force an adversary to retreat from previous gains.
4. *Compel* or *destroy* to impose desired changes to the international security environment and subsequently enforce those outcomes.

To appreciate the breadth and depth of evolving military missions, the range of strategic goals and their associated military tasks must be examined across the *Contexts of Future Conflict*. The set of

[40] George Friedman, *Geopolitical Journey Part 1*, (8 November 2010).

evolving Joint Force missions found in the remainder of *Section 3* is specifically derived by examining the intersection of strategic goals and their associated military tasks with the *Contexts of Future Conflict* (see Figure 5).

Figure 5. Enduring Strategic Goals, Military Tasks, and Contexts of Future Conflict

These missions are not prioritized nor do they indicate the particular likelihood the Joint Force will conduct any one of them. However, as a set, the missions provide a basis for a more detailed discussion about the operational approaches and capabilities that the future Joint Force may require to successfully address *contested norms* and *persistent disorder* within the future security environment.

Adapt to Changing Conditions

In the future, the United States may choose to manage or be compelled to cope with certain security challenges rather than comprehensively solve them. In these situations, the Joint Force will seek to limit the consequences of disruptions to an orderly global security environment. When the United States must adapt to changing conditions, the military tasks associated with this enduring strategic goal are:

- *Shape*. To employ the Joint Force to influence the course of events or to mitigate the negative consequences of competitor initiatives or successes.

- *Contain*. To employ the Joint Force to check the spread of adversary influence and control – or halt the negative consequences of state failure.

While the United States is neither interested in (nor capable of) resisting, countering, or stopping all violent political action that may occur around the world, the Joint Force must be prepared to contain local or limited conflicts or shape transregional and global issues, so they do not deteriorate into larger, more consequential ones. In these cases, the Joint Force will conduct missions designed to shape or contain emerging or chronic challenges within security environment. Figure 6 illustrates the potential missions the future Joint Force may conduct to shape or contain.

Figure 6. Missions to Shape and Contain

Evolving Missions to Shape or Contain

The Joint Force must be prepared to conduct *Global Influence* to understand and blunt adversary use of ideas, images, and violence designed to manipulate the United States and its allies. This should include persistent intelligence and data collection operations to identify active ideological networks and properly classify their motivations, structure, and relationships. The Joint Force will require a close linkage between ongoing information operations against adversary networks and the discrete application of lethal strikes and protective, defensive efforts to reinforce broader national counter-narratives designed to protect, strengthen, and promote free and open societies. This mission entails a degree of cultural and social understanding but also the technical capabilities to listen, analyze, and process information over dynamic, encrypted networks. However, rather than expensive and potentially risky investments by the Joint Force in cultural expertise, containing violent ideologies might better rely on the fusion of U.S. technical capabilities with the human and cultural expertise provided by foreign partners.

The threat of destructive and violent operations on U.S. soil will be a persistent reality in the future security environment. The future Joint Force is likely to play an important role to minimize the consequences of attacks on the United States or its embassies abroad. Therefore, it must be prepared to conduct *Consequence Management* to credibly demonstrate the ability of the United States to overcome attacks against the homeland and sovereign territories. This will include providing assured communications, logistics, ISR, personnel recovery, and engineering capabilities to law enforcement and civil authorities in response to foreign-sponsored attacks against critical infrastructure, civilian populations, or cultural landmarks. In extreme cases, the Joint Force will be required to mitigate the effects of WMD attacks within the United States by providing specialized CBRN capabilities, to include the characterization of biological and chemical agents, and personnel and infrastructure decontamination.

In the future, several aggressive states will challenge the U.S. system of alliances and partnerships, or seek to successfully change international rules in their favor. Consequently, the Joint Force must be prepared to provide *Military Support to Alliances and International Law*. For this mission, the Joint Force should reinforce existing or support the development of new alliances and partnerships in anticipation of adversary initiatives. This might include the ability to understand adversary

objectives relative to the norms and rules they wish to change and inform U.S. leaders how they are being challenged by force or comprehensive stratagem. These operations should include the close pairing of precise situational awareness capabilities with information warfare or public messaging to influence targeted audiences – and broader global populations. Additionally, the Joint Force should be prepared to conduct a range of security cooperation activities to include military engagements, joint exercises, and perhaps new basing and joint support arrangements. This might also include working with competitor states – potentially China, Russia, Iran, and others – in order to shape and influence their initiatives.

The Joint Force must be prepared to conduct *Freedom of Navigation and Overflight* in the global commons to directly support open international norms and to indirectly challenge the initiatives of competitors, particularly in areas where they might have significant military advantages such as the maritime spaces close to their borders or within jammed EMS environments. Specifically, the Joint Force may conduct ambiguous actions and deception operations with low-signature assets to avoid direct confrontation with a competitor, while still demonstrating U.S. resolve to use and keep open the commons for military and civilian purposes. In parts of the commons militarily contested by adversaries, the Joint Force should encourage preferred rules and norms through a range of information and sensor warfare operations designed to confuse adversaries, avoid triggers for more open conflict, and force the misallocation of military resources by competitors. Furthermore, this mission is likely to involve international stakeholders so the Joint Force should be prepared to work closely with allies and partners.

The future security environment will continue to feature a range of adversaries attempting to shape political behavior by conducting damaging or disruptive cyber-attacks. The Joint Force must minimize the consequences of threatened or successful cyberattacks against the United States, its allies, and partners by conducting *Military Support to Cyber Resiliency*. This mission will require cyber support to U.S. government and civilian organizations, allied nations, and other international partners that credibly reinforces the resilience of cyber-dependent systems and infrastructure. This includes a capacity to reliably communicate, compute, store, and retrieve critical data that outpaces adversary efforts to deny these capabilities. Furthermore, the Joint Force should develop the capacity to work with a range of nontraditional partners such as private companies or cyber activists to offset adversary operations in cyberspace, for example, by identifying and interdicting adversary cyber operatives.

The future security environment will present humanitarian catastrophes on a scale that may dwarf the ability of the United States to completely address all of the associated negative consequences. However, the Joint Force must be prepared to conduct *Noncombatant Evacuation and Foreign Humanitarian Assistance* in order to protect U.S. citizens or relieve the worst suffering from a deteriorating security situation. Here, the Joint Force must first limit U.S. exposure to threats emanating from a failed or failing state by protecting or evacuating U.S. citizens and by defending key facilities in semi-opposed or opposed environments, often within powerful A2/AD and guided rocket, artillery, missile, and mortar (G-RAMM) envelopes. Furthermore, the Joint Force may conduct operations to encourage neighboring states to limit the spread of disorder from a failed or failing state, such as providing assistance with the management of refugee movements and dispositions. Finally, some shattered states may feature the intentional use or accidental release of

chemical, biological, radiological, or nuclear weapons. In these cases, the Joint Force may be required to mitigate the effects of WMD use in the midst of a civil or international conflict.

Manage Antagonism and Impose Costs

There will be instances when the United States will resolve to oppose the aggressive activities of state and non-state actors – whether overt, covert, or a hybrid mix. In these cases, the Joint Force will be required to more actively and forcefully resist adversaries and discourage unfavorable changes to the security environment. When the United States decides to manage an antagonistic competitor or impose costs on adversary courses of action, the military tasks associated with this enduring strategic goal are:

- *Deter*. To employ the Joint Force to prevent or discourage adversary action.
- *Deny*. To employ the Joint Force to refuse adversary use of an already seized or controlled objective.

The Joint Force must be prepared to protect and defend key U.S. interests against adversaries who attempt to shape or otherwise alter the security environment at the expense of the United States or its allies. Consequently, the future Joint Force will conduct missions to deter or deny adversaries from engaging in coercive strategies or benefiting from conflict and war by raising the potential costs of their actions above what they are prepared to bear. Figure 7 illustrates the potential missions the future Joint Force may conduct to deter or deny.

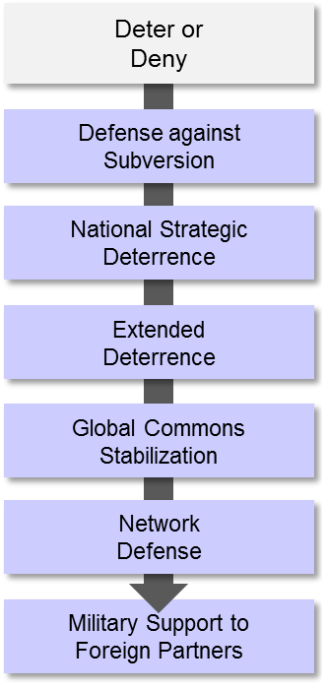

Figure 7. Missions to Deter or Deny

Evolving Missions to Deter or Deny

The Joint Force must be prepared to conduct *Defense against Subversion*. These missions will discourage both state and non-state ideological networks from taking political and military actions to undermine the military, economic, psychological, or political strength or morale of the United States, its allies and partners. They will feature an integrated mix of global activities and local operations to strengthen and protect the stability and integrity of key foreign partners. Initially, information operations designed to weaken adversary initiatives by encouraging local competition among existing ideological networks will simultaneously motivate local resistance to competitor networks. Furthermore, to counter the wide ranging subversive efforts of states and terrorist groups, the Joint Force may conduct synchronized and coordinated Foreign Internal Defense, Security Force Assistance, and potentially unconventional warfare across several threatened states and jurisdictions. This mission should focus on denying adversaries visible victories and demonstrating the capacity to reject their desired objectives.

The foundation for U.S. survival in a world of nuclear states is the credible capability to hold other nuclear great powers at risk, which will be complicated by the emergence of more capable, survivable, and numerous competitor nuclear forces. Therefore, the future Joint Force must be prepared to conduct *National Strategic Deterrence*. This includes leveraging layered missile defenses to complicate adversary nuclear planning; fielding U.S. nuclear forces capable of threatening the leadership, military forces, and industrial and economic assets of potential

adversaries; and demonstrating the readiness of these forces through exercises and other flexible deterrent operations. The Joint Force must also deter state and non-state adversaries from pursuing terrorist attacks against the homeland. This will likely feature intelligence and data collection with domestic agencies and international partners to identify and track domestic terrorists combined with the use of punitive strikes and raids to disconnect them from their sources of foreign support.

As a number of states seek to extend their power and influence more broadly, they are likely to threaten U.S. global interests and commitments around the world. The Joint Force must be prepared to conduct *Extended Deterrence* to assure allies and partners and to raise the cost to adversaries who threaten critical national interests. Assurance and deterrence in a world of many capable regional powers will require the Joint Force to apply active and passive security measures, including the development of credible expeditionary and power projection capabilities, protected forward basing, joint nuclear assurance missions, and a range of fixed and deployable military presence postures. In the future, the Joint Force should be capable of reducing the likelihood or impact of coercive diplomacy that seeks to exclude U.S. influence or access. Specifically, the force should be prepared to cooperate with allies to preempt competitor initiatives or prevent threats from expanding through combined Foreign Internal Defense, Security Force Assistance, unconventional warfare, and show of force operations directed against an aggressive adversary.

The Joint Force must be prepared to conduct *Global Commons Stabilization* to deter adversaries from contesting free use of the seas, air, space, and electromagnetic spectrum. These missions will hinge on a Joint Force capable of conducting intelligence operations with allies and partners to develop awareness of competitor activities in the commons including establishing a common operating picture, but also identifying and analyzing trends with advanced pattern recognition capabilities to better understand the difference between regular traffic and impending military closure or interdiction. Furthermore, the Joint Force must be capable of protecting national objectives in the global commons despite the use of asymmetric, unconventional, and hybrid approaches by competitors to assert new claims and exercise more control in the commons. This will require operations that impose costs on adversaries who impede free use of the commons, such as targeted electromagnetic and space denial measures, the enforcement of sanctions, or the establishment of electromagnetic exclusion zones.

As more devices, systems, and national infrastructure are connected to cyberspace, critical systems will be targeted by adversary cyber weapons. In order to deter adversaries from violating U.S. interests in cyberspace and deny their ability to interdict critical U.S. cyber systems, the future Joint Force must be prepared to conduct national and allied *Network Defense*. These missions will require steady-state information operations in support of national cyber deterrence strategies that communicate the resiliency of critical U.S. systems and infrastructure, while protecting their vulnerabilities. Key actions may include the development of a Department of Defense cyber umbrella; the creation of a national "cyber border patrol;" more comprehensive intelligence sharing efforts; contributions to national level cyber exercises; the development of hardened networks; and reinforced coordination with domestic law enforcement.

The future security environment will feature adversaries undermining the integrity of states or taking advantage of a state that is failing. The Joint Force must be prepared to conduct *Military Support to Foreign Partners* to bolster or reinforce the government of a failing state. During these

missions, the Joint Force might conduct unconventional warfare, working with and through host nation partners, to support the reestablishment of domestic order, including the use of technical and human capabilities to identify, track, and isolate foreign agents and proxies. Furthermore, the Joint Force may conduct peacekeeping operations to separate combatants or to protect at-risk populations, including the creation of no fly zones or humanitarian safe zones. The Joint Force should also be prepared to preempt terrorist, insurgent, or criminal groups attempting to obtain chemical, biological, radiological, or even nuclear weapons in a collapsing state. The Joint Force might be required to conduct operations in potentially denied areas to neutralize, seize, secure, and render safe fissile materials and warheads, and chemical/biological agents and precursors.

Punish Aggression and Rollback Gains

The United States may determine it is necessary to take back or offset gains by adversaries attempting to change the international system through violence. Therefore, the Joint Force must be capable of blocking adversary courses of action, exacting consequences for their aggression, and impeding their ability to continue pursuing offensive or coercive activities. When the United States decides it must punish an aggressor or rollback adversary gains, the military tasks associated with this enduring strategic goal are:

- *Disrupt*. To employ the Joint Force to interrupt or impede the progress of adversary initiatives, including retaking adversary objectives.
- *Degrade*. To employ the Joint Force to lower in quality or value the capabilities and possessions of adversaries.

The future Joint Force will conduct missions designed to disrupt an adversary's ability to pursue unfavorable changes to the security environment or physically degrade their capacity to secure objectives. Furthermore, it must do this against competitors with very large and capable militaries, that are often sheltered under a nuclear umbrella, protected by other political or military factors, concealed by dispersed networks, or operate amongst the people. Figure 8 illustrates the potential missions the future Joint Force may conduct to disrupt or degrade.

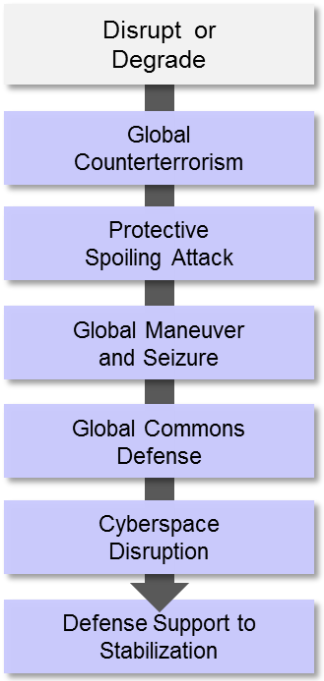

Figure 8. Missions to Disrupt or Degrade

Evolving Missions to Disrupt or Degrade

The Joint Force must be prepared to conduct *Global Counterterrorism* to disrupt violent ideological organizations or degrade their ability to threaten U.S. interests. This will include intelligence and data collection operations to identify and understand what adversary networks value and steady-state offensive cyber operations to erode their ability to coordinate activities. Additionally, the future Joint Force will leverage persistent surveillance and strike operations against extremist groups to desynchronize their operations and temporarily interrupt their use of safe havens. This mission might also include the use of defensive actions to block offensive operations by adversary networks while simultaneously raising their costs to achieve a particular objective, and local or regionally-focused counterinsurgency to eliminate societal sources of support. Furthermore, the Joint Force is likely to conduct operations against violent extremist

groups in politically-sensitive and non-permissive environments, where adversaries have low-tech but effective air defense and other A2/AD capabilities.

The U.S. homeland will be increasingly vulnerable to a wide range of emerging adversary strike capabilities. Therefore, the Joint Force must be prepared to conduct a *Protective Spoiling Attack* in order to disrupt adversary operations against the United States or its citizens and to degrade their ability to credibly threaten both. These missions will include protection of the aerospace and maritime approaches to the United States from hypersonic weapons, highly maneuverable ballistic missiles, stealthy cruise missiles, and small, smart, and autonomous surface and subsurface platforms. Furthermore, the Joint Force must be capable of contributing to the identification and disruption of global terrorist groups, state sponsored proxies, criminal networks, and other threats capable of clandestinely organizing, arming, and operating within the United States. This might include actions to forcibly disconnect these groups from their sources of foreign support, including offensive operations through the electromagnetic spectrum and cyberspace to disorganize and/or interrupt adversary attacks against the homeland.

Future adversaries are likely to conduct offensive operations to seize key objectives, protect gains through advanced A2/AD capabilities, and establish stand-off by leveraging flexible nuclear deterrent capabilities. In these situations, the United States might be inclined to disrupt or degrade countervailing powers or coalitions while avoiding cost-prohibitive, potentially catastrophic escalation. Consequently, the Joint Force must be prepared to conduct *Global Maneuver and Seizure* to defend important interests, retake key terrain, or seize critical objectives captured by an adversary. In these missions, the Joint Force will delay further adversary aggression through defensive actions while simultaneously conducting targeted strikes and raids to disrupt adversary initiatives. To reverse adversary gains, the Joint Force will conduct entry operations, establish lodgments with effective air defense umbrellas, and use other offensive operations to seize terrain from adversaries who will be increasingly capable of assembling very capable military forces. Finally, the Joint Force must prepare for offense operations to rollback adversary gains and restore the status quo.

The Joint Force must be prepared to conduct *Global Commons Defense* to disrupt the ability of adversaries to interdict the seas, air, space, and electromagnetic spectrum, or otherwise degrade an adversary's ability to operate in the commons in ways unfavorable to U.S. interests. These missions might involve the creation of forward-projected, multi-domain blockades to impede adversary use of the commons. The Joint Force will establish these area-denial zones through a flexible combination of surface and subsurface sea control capabilities, air defense measures, offensive space operations, and electronic warfare. This mission is likely to be complicated by an adversary's use of strike assets positioned on sovereign territory or the deceptive placement of sensor systems on commercial platforms, to include space assets. Despite these challenges, the Joint Force must maintain the ability to conduct targeted command and control warfare, counter ISR operations, and discriminate sensor interdiction and spoofing in all commons. Furthermore, the Joint Force should be capable of responding to the threat of adversaries creating debris fields in important orbits. The Joint Force should explore ways to enhance operations in the commons by leveraging anticipated advances in long-range robotic and autonomous systems.

Anticipating that more adversaries around the world, to include both state and non-state actors, will develop advanced capabilities to threaten critical U.S. interests in cyberspace, the Joint Force must be prepared to conduct *Cyberspace Disruption* to attack adversary assets and impede their ability to adversely affect the unrestricted use of cyberspace by the United States. Offensive cyber operations will impose costs on adversaries by identifying and exploiting their cyber vulnerabilities, and may include distributed denial of service attacks, targeted cyber denial measures, and actions to physically impair military systems through cyberspace. Additionally, the Joint Force may conduct proportional cross-domain operations to physically damage an adversary's cyber infrastructure, using weapons operating in other domains to suppress enemy cyber defenses and specifically strike their critical cyber infrastructure. Furthermore, these operations should be coupled with defensive cyber efforts to block adversary responses, and might include the use of autonomous or semi-autonomous cyber defense systems or the activation of war reserve networks when peacetime networks are unavailable.

The future security environment will feature well-organized states or even powerful non-state entities seeking to take advantage of weak and fragile states. In certain situations, the United States might want to prevent an adversary from violating the integrity of a state or block an adversary from benefitting from an already shattered state or region. Therefore, the Joint Force may conduct *Defense Support to Stabilization* to disrupt an adversary attempting to take advantage of a disordered state or region. These missions might focus on strengthening local partners by isolating and degrading adversary proxy forces through unconventional warfare or targeted strikes and raids. Furthermore, the Joint Force might conduct blocking operations designed to impede the sources of external influence, control, and support to local proxies. This may include the enforcement of multi-domain exclusion zones, the use of cross-border punitive raids, or military support to a local resistance movement opposing the targeted adversary. Finally, these missions may also include activities to prevent adversaries from seizing and using fissile materials and warheads, and chemical/biological agents and precursors.

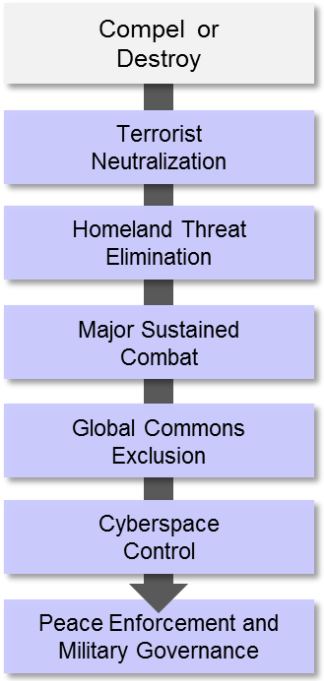

Figure 9. Missions to Compel or Destroy

Impose Change and Enforce Outcomes

In the most dangerous cases, some adversaries will pursue strategic goals that are intolerable to the United States. In these cases, the Joint Force will force compliance by adversaries to a new and sustainable equilibrium protected by the United States, its allies, and partners. When the United States decides to impose change and enforce preferred outcomes, the military tasks associated with this enduring strategic goal are:

- *Compel*. To employ the Joint Force to force an adversary to mentally or physically submit to U.S. preferences, priorities, and arrangements.
- *Destroy*. To employ the Joint Force to render adversary capabilities physically unusable or to cause its political or military structures to cease to exist as a distinguishable entity.

The Joint Force must be prepared to fully defeat adversaries directly threatening the United States or the global system of allies, rules, and norms that it supports by ensuring that they are no longer willing or able to present a threat to U.S. interests. Consequently, the Joint Force will

conduct missions designed to compel adversaries or destroy their physical capacity to resist preferred U.S. political outcomes. Figure 9 illustrates the potential missions the future Joint Force may conduct to compel or destroy.

Evolving Missions to Compel or Destroy

In the future security environment, the United States might decide that a particularly virulent and violent organization with totalitarian or genocidal goals is incompatible with the existence or safety of free societies. In these cases, the Joint Force must be prepared to conduct comprehensive *Terrorist Neutralization* in order to destroy a violent identity network or compel it to forgo violence in support of their political objectives. The mission to destroy terrorist groups and neutralize their ideological aspirations will involve multiple, simultaneous, and global counterterrorism operations integrated with law enforcement efforts and national messaging initiatives. The Joint Force must have the capacity to conduct wide ranging, sustained offensive operations to render the capabilities of adversary networks physically unusable and permanently eradicate adversary safe havens. In certain areas, the Joint Force may also conduct counterinsurgency operations and military governance across multiple regions to eradicate the military and political structures of adversary networks.

Future adversaries may threaten the United States with imminent WMD or other conventional attacks against its homeland or citizens. Such an attack, particularly with one or more nuclear devices, would present an exceptionally grave threat to national security. As such, the Joint Force must be prepared to conduct *Homeland Threat Elimination* to terminate the capacity of adversaries to strike the U.S. homeland, and later compel them to accept U.S. terms of capitulation. These missions will require prompt global strike capabilities and a range of forward-based assets to engage and destroy adversary air, sea, and land forces capable of reaching the U.S. homeland. This includes the ability for the Joint Force to fight through the deterrent strategies of nuclear-capable adversaries. In extreme cases, the Joint Force might be called on to combat adversary forces operating within the homeland by augmenting law enforcement, or in the worst case, via major combat operations should adversary forces breach U.S. sovereign borders or seize U.S. territory.

A future state or coalition of states may – through weakness or overreach – launch operations to inflict the greatest damage possible against the United States and its global interests. In such cases, the Joint Force must be prepared to conduct *Major Sustained Combat* to destroy a countervailing power, alliance, or partnership or compel them to recognize U.S. interests. These missions should seize the initiative by reducing adversary defenses at range, followed by the use of speedy, targeted offensive actions to destroy adversary global and regional strike assets, to include nuclear capabilities. Combined offensive operations will then be required to seize key terrain from adversaries and permanently eradicate resistance. These campaigns must account for the global presence and influence of powerful adversaries, and they may be multi-year conflicts that are unlikely to be won quickly or cheaply. Eventually, the Joint Force may engage in military governance to impose U.S. preferred political and military structures on adversary territory, including post-conflict reconstruction and assistance.

In certain situations where adversaries pose intolerable threats to the global commons, the United States may elect to disconnect them from one or more of the commons and eliminate their ability to influence these domains. The Joint Force must be prepared to conduct *Global Commons*

Exclusion in order to enforce open and free use of the seas, air, space, and electromagnetic spectrum and compel the recognition of U.S. favored norms and rules within them. This will likely include multi-domain offensive operations using coordinated and simultaneous electronic, cyber, space, and kinetic actions to eradicate adversary capabilities that can influence or affect the commons. Concurrently, the Joint Force may launch operations to force the withdrawal of adversaries from the commons by damaging critical assets including attacks on launch facilities; economic and financial nodes; position, navigation and timing satellites; naval vessels; and land-based aerial strike assets. The Joint Force must also protect the commons and enforce U.S. preferred norms through a range of convoy operations, integrated air and missile defenses, maritime mine warfare, and subsurface combat.

Cyberspace provides an avenue to inflict severe damage on the United States by manipulating networks, the machines connected to networks, and the ideas transmitted over them. In many cases, the use of cyber coercion against the United States will be intolerable. Therefore, the Joint Force must be prepared to conduct *Cyberspace Control* to eliminate an adversary's ability to define and defend their interests in cyberspace and force them to recognize U.S. views on its use. Cyberspace control operations will frequently integrate cyber and non-cyber capabilities. In coordination with law enforcement agencies, offensive operations may be required to identify, target, and capture or kill adversary cyber operatives. Offensive operations will also be used to eradicate an adversary's cyber infrastructure and capabilities, which might include an array of kinetic strikes combined with simultaneous electronic, cyber, and space warfare actions. Finally, the Joint Force may impose cyber-military governance, including the introduction of U.S. cyber rules and laws on captured adversary networks to include the control of domain names, access and registration, and administration of key systems.

The consequences of state or regional failure may be so dire that the United States decides to impose an enduring and stable order. Consequently, the Joint Force must be prepared to conduct *Peace Enforcement and Military Governance* to destroy an insurgent force resisting a legitimate government or to compel an external adversary to recognize the integrity and authority of a particular state. This might include counterinsurgency operations to eliminate local resistance to state authority, taking advantage of advanced biometric capabilities, big data pattern recognition, and persistent ISR to support the separation of combatants from noncombatants. The Joint Force may also conduct peace enforcement operations to terminate a conflict and impose compliance with an internationally recognized settlement. Both counterinsurgency and peace enforcement will include stability operations, and perhaps limited military governance, to restore the political authority of a state or multiple states. Above all, the Joint Force should have the capacity to deploy a historically-grounded ratio of forces to governed populations if called upon to decisively restore a failed or failing state, or develop capabilities that effectively replicate these ratios (for example, remotely piloted or autonomous infantry/patrol robotic systems).

Summary

This section described a range of evolving missions that the future Joint Force may be required to conduct in 2035. The missions presented at the intersection of U.S. strategic goals with the disparate *Contexts of Future Conflict* should not be viewed as a clearly defined, precise, and discrete set. Rather, they should be viewed as a potential vocabulary for the inevitable strategic dialogue that must occur between future military planners and their political leadership.

To secure the broadest interests of our Nation, political leaders will demand real options from their military. In turn, military leaders require clear strategic guidance and assurance that political leaders understand what military power can feasibly achieve and the consequences of using military power. This range of missions is a start point for that future dialogue – a dialogue whose outcome is shaped by the force development activities of today (see Figure 10).

Figure 10. Evolving Joint Force Missions

It is unclear whether the future Joint Force can be proficient at employing military force across this entire mission set to simultaneously and effectively address *contested norms* and counter *persistent disorder* with currently projected capabilities, operational approaches, and fiscal resources. Military investments to prepare for the future security environment require consequential decisions about relative priorities and possible risk. Further, these decisions must be based on the ability to assess, frustrate, and defeat opposing military *strategies* which first requires an understanding of why nations and groups take the momentous decision to go to war.

Placing too much emphasis on *contested norms* – particularly those high-tech and expensive capabilities geared to contain or disrupt an expansionist state power – may discount potentially disruptive low-end threats, which have demonstrated a troubling tendency to fester and emerge as surprise or strategic shock for the United States. Conversely, tilting the balance of force development activities towards capabilities designed to counter *persistent disorder* may risk a world in which other great powers or alliances of great powers decisively shift the international order in ways highly unfavorable to the United States, its allies, and partners.

Conclusion

> *"The primary purpose of any theory is to clarify concepts and ideas that have become, as it were, confused and entangled."*[41]

Although war is itself an enduring feature of the human condition, the character of war is always evolving. This change in the character of war demands our attention. The emerging security environment can be described by simultaneous and connected challenges – *contested norms* and *persistent disorder*. The evolution of these challenges in the security environment of 2035 will be evident across *World Order*; *Human Geography*; and *Science, Technology, and Engineering*.

Competitor states and some powerful non-state actors will challenge the rules that underpin the current global order. Meanwhile, fragile states will become increasingly incapable of maintaining order. Moreover, anticipated scientific and technical advances will likely lead to greater parity among a range of international actors thus allowing potential adversaries to more effectively challenge U.S. global interests.

Trends and conditions will converge and intersect, creating six specific *Contexts of Future Conflict* that describe the character of future conflict, the nature of potential adversaries, and the characteristics of the military competitive space. Future conflict will feature more capable adversaries placing difficult demands on the Joint Force over wide areas of the globe. Furthermore, the effectiveness and sustainability of Joint Force operations over time will be highly dependent on popular perceptions, attitudes, and broad acceptance of their legitimacy.

When linked to an understanding of the potential range of future U.S. strategic goals and enduring military tasks, the *Contexts of Future Conflict* enable the identification of likely Joint Force missions. The scope of these missions reflects the need to simultaneously address high-end threats to favorable global order with the need to confront disruptive low-end threats emerging from a disordered world. However, the missions should not be viewed as a clearly defined, precise, and discrete set, but rather, a start point for a dialogue between military planners and their political leaders.

The outcome of this dialogue will be shaped by the force development activities of today. It is unclear whether the Joint Force can be simultaneously proficient at addressing *contested norms* and *persistent disorder* with currently projected capabilities, operational approaches, and fiscal resources. Therefore, the United States must consider military investments that acknowledge there may be times when it is more appropriate to manage global security problems as opposed to undertaking expensive efforts to comprehensively solve them.

JOE 2035 is designed to encourage the purposeful preparation of the Joint Force to effectively manage this reality. It sets the stage for a more detailed conversation about **how** the Joint Force can achieve success in the future security environment. *JOE 2035* was written to accelerate new ways – or concepts – for the Joint Force to address the likely needs of future strategy and thus, identify a foundation upon which enduring U.S. military advantages can be built.

---

[41] Carl Von Clausewitz, *On War*. (trans. Paret and Howard, 1976/1984), p. 132.