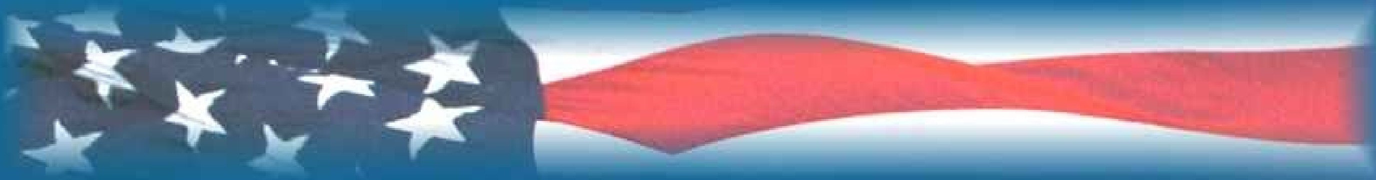


Foundations for Innovation

Strategic R&D Opportunities for 21st Century Cyber-Physical Systems

Connecting Computer and Information Systems With the Physical World

Robots, Autonomous Vehicles

Progressive Management

Foundations for Innovation: Strategic R&D Opportunities for 21st Century Cyber-Physical Systems - Connecting Computer and Information Systems With the Physical World, Robots, Autonomous Vehicles

* * * * * * * * * * * * *

U.S. Government, National Institute of Standards and Technology

* * * * * * * * * * * * *

Progressive Management

Questions? Suggestions? Comments? Concerns? Please contact the publisher directly at

bookcustomerservice@gmail.com

Remember, the book retailer can’t answer your questions, but we can!

* * * * * * * * * * * * *

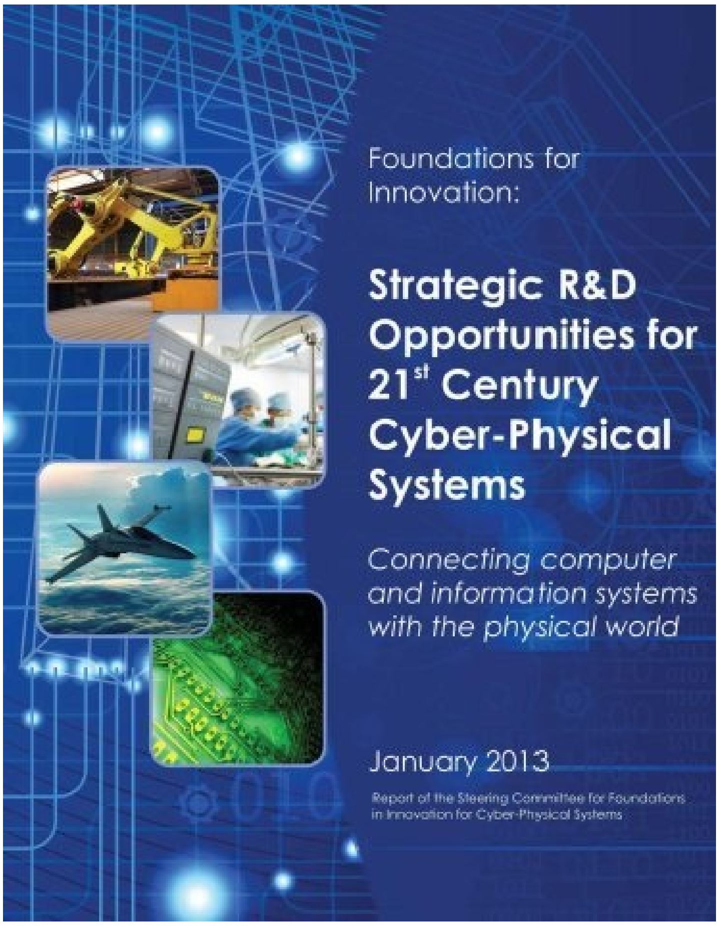
This is a privately authored news service and educational publication of Progressive Management. Our publications synthesize official government information with original material - they are not produced by the federal government. They are designed to provide a convenient user-friendly reference work to uniformly present authoritative knowledge that can be rapidly read, reviewed or searched. Vast archives of important data that might otherwise remain inaccessible are available for instant review no matter where you are. This e-book format makes a great reference work and educational tool. There is no other reference book that is as convenient, comprehensive, thoroughly researched, and portable - everything you need to know, from renowned experts you trust. For over a quarter of a century, our news, educational, technical, scientific, and medical publications have made unique and valuable references accessible to all people. Our e-books put knowledge at your fingertips, and an expert in your pocket!

* * * * * * * * * * * * *

CONTENTS

* * * * * * * * * * * * *

* * * * * * * * * * * * *



Foundations for
Innovation:

Strategic R&D
Opportunities for
21st Century
Cyber-Physical
Systems

*Connecting computer
and information systems
with the physical world*

January 2013

Report of the Steering Committee for Foundations
in Innovation for Cyber-Physical Systems

Foundations for Innovation: Strategic R&D Opportunities for 21st Century Cyber-Physical Systems - Connecting Computer and Information Systems With the Physical World

January 2013

Report of the Steering Committee for Foundations in Innovation for Cyber-Physical Systems

* * * * * * * * * * * *

STEERING COMMITTEE FOR FOUNDATIONS FOR INNOVATION IN CYBER-PHYSICAL SYSTEMS

This report was prepared through the collaborative efforts of the individuals noted below. It reflects their expert contributions as well as the many insights generated at the Foundations for Innovation in Cyber-Physical Systems Workshop held March 13-14, 2012 in Rosemont, Illinois.

Committee Co-chairs

Janos Sztipanovits, Vanderbilt University

Susan Ying, Boeing

Steering Committee Members

Isaac Cohen, United Technologies Corporations

David Corman, Boeing

Jim Davis, UCLA and Smart Manufacturing Leadership Coalition

Himanshu Khurana, Honeywell Automation and Control Solutions

Pieter J. Mosterman, MathWorks

Venkatesh Prasad, Ford

Lonny Stormo, Medtronic, Inc.

This report was prepared as an account of work cosponsored by the National Institute of Standards and Technology (NIST). The views and opinions expressed herein do not necessarily state or reflect those of NIST. Certain commercial entities, equipment, or materials may be identified in this document in order to illustrate a point or concept. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

* * * * * * * * * * * * *

CONTRIBUTORS

Yiannis Aloimonos, University of Maryland, College Park

Carl Andersen, Federal Highway Administration

John Banting, Cooper Power Systems

Jay Bayne, Milwaukee Institute

Aaron Becker, University of Illinois, Urbana-Champaign

Patrick Beeson, Traclabs, Inc.

Aaron Bobick, Georgia Institute of Technology

Justin Bradley, University of Michigan

Brent Brunell, General Electric

Jason Burt, Bonneville Power Administration

David Chilin, University of California, Los Angeles

George Chiu, National Science Foundation

Isaac Cohen, United Technologies Corporation

Mike Coop, ThinkSmartGrid

David Corman, Boeing

Stephen Craven, University of Tennessee, Chattanooga

Joe D’Ambrosio, General Motors

Jim Davis, UCLA and Smart Manufacturing Leadership Coalition

Kent Donohue, UL LLC

Bruce Douglass, IBM

Sameh Elsharkawy, NiLogix, Inc.

Yaser P. Fallah, West Virginia University

Aydin Farajidavar, Georgia Institute of Technology

Kathleen Fisher, Defense Advanced Research Projects Agency

Tom Fuhrman, General Motors

Christopher Geyer, iRobot Corporation

Maysam Ghovanloo, Georgia Institute of Technology

Christopher Gill, Washington University in St. Louis

Helen Gill, National Science Foundation

Julian Goldman, Massachusetts General Hospital/Harvard Medical School

Bill Goodwine, University of Notre Dame

Chetan Gupta, HP Labs

Donny Helm, Oncor Electric Delivery

Naira Hovakimyan, University of Illinois, Urbana-Champaign

David Johnson, Boston Scientific

David Knowles, University of North Carolina,
Chapel Hill

Heath LeBlanc, Vanderbilt University

Edward Lee, University of California, Berkeley

Hongwei Liao, University of Michigan

Taylor Lochrane, Federal Highway Administration

Amin Maghareh, Purdue University

Mary Ann Maher, SoftMEMS

Keith Marzullo, National Science Foundation

Eamonn McCormick, Alvarez and Marsal

Pieter J. Mosterman, MathWorks

Brian Murray, United Technologies Research Center

Necmiye Ozay, California Institute of Technology

Umit Ozguner, Ohio State University

Taskin Padir, Worcester Polytechnic Institute

Sai Prathyusha Peddi, The Ohio State University

Linh ThiXuan Phan, University of Pennsylvania

Lee Pike, Galois, Inc.

Radha Poovendran, University of Washington

Leonard Radtke, Medtronic

Wenjing Rao, University of Illinois at Chicago

Luiz Rust Carmo, Inmetro Brazil

Bill Sanders, University of Illinois

Chaitanya Sankavaram, University of Connecticut

Shankar Sastry, University of California, Berkeley

A. Prasad Sistla, University of Illinois at Chicago

Jonathan Sprinkle, University of Arizona

Gaurav Srivastava, University at Buffalo

Anthony Star, Illinois Commerce Commission

Zhuoxiong Sun, Purdue University

James Swanson, University of Cincinnati

Janos Sztipanovits, Vanderbilt University

Burt Theurer, General Electric Global Research

David Vasko, Rockwell Automation

Ceeman Vellaithurai, Washington State University

Krishna Venkatasubramanian, University of Pennsylvania

Philip Wilsey, University of Cincinnati

Alexander Wyglinski, Worcester Polytechnic Institute

Mumu Xu, California Institute of Technology

Shahan Yang, University of Maryland

Susan Ying, Boeing

Justyna Zander, Harvard University, Simulated Way

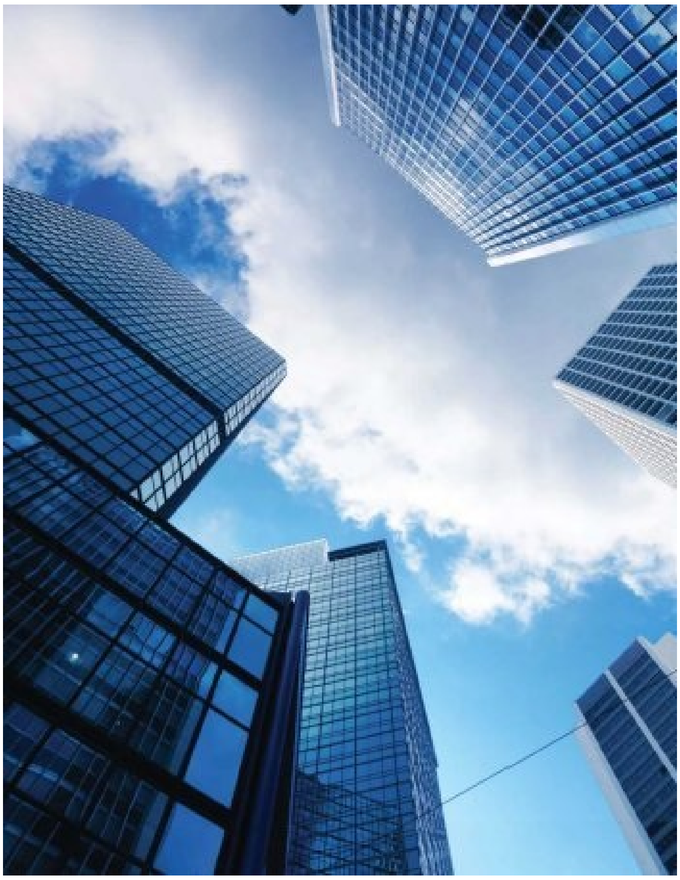
Hongwei Zhang, Wayne State University

Feng Zhao, Microsoft Research-Asia

Lei Zhao, Purdue University

Yi Zhao, Futurewei

Hao Zheng, University of South Florida



CONTENTS

This report is the third in a series of reports developed with input from a group of world-renowned experts in cyber-physical systems (CPS) and related technologies. The first in the series is the Foundations for Innovation in Cyber-Physical Systems Workshop Report, which summarizes the results of a workshop held in March 2012 to gain broad views on the technology and measurement challenges limiting CPS. Second in the series is Strategic Vision and Business Drivers for 21st Century Cyber-Physical Systems, a report summarizing the ideas generated by a June 2012 Executive Roundtable. This event was attended by business and technical leaders in the field representing a spectrum of applications for CPS, from medicine to energy to manufacturing.

Building on previous reports, this document provides a high-level perspective of the key challenges and strategic research and development opportunities for advancing CPS. The report will be used by both public and private stakeholders to inform decisions about the technology R&D that should be pursued, as well as the new measurement methods and standards that must be developed to realize the transformative potential of CPS.

INTRODUCTION

The wide reach of the Internet along with rapid advances in miniaturization, speed, power, and mobility have led to the pervasive use of networking and information technologies (IT) across all economic sectors. Increasingly, these technologies are combined with elements of the physical world (e.g., machines, devices, structures) to create smart or intelligent systems that offer increased effectiveness, productivity, safety, and speed and enable functions not previously possible.

Integrated networking, information processing, sensing and actuation capabilities allow physical devices to operate in changing environments. This makes smart systems possible but also creates the need for a new ‘systems science’ that can lead to unprecedented capabilities. Tightly coupled cyber and physical systems that exhibit this level of integrated intelligence are sometimes referred to as cyber-physical systems (CPS). All CPS have computational processes that interact with physical components. These can be relatively simple (e.g., a heater, cutting machine) or comprise multiple components in complex assemblies (e.g., vehicles, aircraft systems, oil refineries). The computational and physical processes of such systems are tightly interconnected and coordinated to work together effectively, often with humans in the loop.

Robots, intelligent buildings, implantable medical devices, cars that drive themselves or planes that automatically fly in a controlled airspace—these are all examples of CPS. Today, CPS can be found in such diverse industries as aerospace, automotive, energy, healthcare, manufacturing, infrastructure, consumer electronics, and communications. Everyday life is becoming increasingly dependent on these systems—in some cases with dramatic improvements.

There is a growing trend toward computational intelligence, automation, and control for complicated but well-defined tasks or processes, especially when demands or constraints are not amenable to human intervention. For example, automatic collision systems could detect moving objects and respond faster than a human operator. Unmanned CPS could be used to reduce the risk to human life by detecting mines, exploring volcanoes, or conducting otherwise hazardous tasks. Machines driven by a computer do not suffer fatigue and may be more precise than is humanly possible. In future CPS could make possible concepts only imagined today, such as unmanned tours to the moon, bionic suits, and automated large-scale indoor agriculture systems.

This trend does not remove the importance of human involvement but does change roles and requirements for new skill sets. Furthermore, as CPS become more dependent on computational processes, it becomes increasingly important that they be engineered to be reliable, secure, and safe. Future scientific and engineering advances that extend the connectivity of these systems and deliver greater reliability could open new opportunities to take advantage of the unique properties of CPS.

A CALL TO ACTION

The future applications of CPS are more transformative than the IT revolution of the past three decades. Unparalleled analytical capabilities, real-time networked information, and pervasive sensing, actuating, and computation are creating powerful opportunities for systems integration. Next generation CPS will be able to execute extraordinary tasks that are barely imagined today. These new capabilities will require high-confidence computing systems that can interact appropriately with humans and the physical world in dynamic environments and under unforeseen conditions. Achieving these capabilities presents a complex and multi-disciplinary engineering challenge.

Future CPS have many sophisticated, interconnected parts that must instantaneously exchange, parse, and act on detailed data in a highly coordinated manner. Continued advances in science and engineering will be necessary to enable advances in design and development of these complex systems. Multi-scale, multi-layer, multi-domain, and multi-system integrated infrastructures will require new foundations in system science and engineering. Scientists with an understanding of otherwise physical systems will need to work in tandem with computer and information scientists to achieve effective, workable designs. Standards and protocols will be necessary to help ensure that all interfaces between components are both composable and interoperable, while behaving in a predictable, reliable way.

This report is a call to action. It outlines a set of strategic R&D opportunities that must be addressed to enable advanced CPS to reach their potential and deliver broad societal benefits in the future. The United States (U.S.) is a global leader in cyber technologies and well-positioned to gain a competitive advantage in CPS. Work in CPS is moving rapidly forward on a global scale. In the European Union, the ARTEMIS program has proposed spending $7 billion on embedded systems and CPS by 2013—with a view to becoming a global leader in the field by 2020. Japan is capitalizing on its traditional strengths in this field to make technology advances, and currently hosts the largest tradeshow in the world on embedded systems. The great potential of CPS is motivating countries such as India and China to forge ahead into the field. The opportunity is now for the U.S. to establish competitive leadership through the ability to develop next generation systems that you can trust your life with.

“Advanced sensing, measurement, and process control, including cyber-physical systems… has applicability across almost all industry domains. These technologies are critical for enhancing tradability. megatrends of energy and resource efficiency, better safety, and higher quality also depend highly on advances in sensing and automatic process control.”

Recommendation #2, Increase R&D Funding in Top Cross-cutting Technologies, from the Report to the President on Capturing Domestic Competitive Advantage in Advanced Manufacturing (PCAST, 2012)

REAPING THE BENEFITS OF CYBER-PHYSICAL SYSTEMS

Development and use of advanced CPS will generate unique opportunities for economic growth, create skilled jobs for the long term, and help ensure the health, safety, and security of the nation while improving quality of life. CPS are drivers for innovation in a broad range of industries and can lead to new products or unlock new markets (see Table 1). By the end of the decade, embedded networking and computing components are projected to account for more than half of the value share in diverse sectors, including automotive, consumer electronics, avionics and aerospace, manufacturing, telecommunications, intelligent buildings, and health and medical equipment. A recent report estimates that the technical innovations of CPS could find direct application in sectors currently accounting for more than $32.3 trillion in economic activity, and with the potential to grow to $82 trillion of output by 2025—about one half of the global economy (GE, 2012).

U.S. manufacturing competitiveness will increasingly rely upon CPS technologies for advanced robotics and computer-controlled manufacturing processes linked to automated design tools, along with integrated, broad-based, and dynamic management of production lines, factories, and supply chains. Equally broad-based performance metrics will be needed to enable integration of economic, productivity, energy, and sustainability objectives.

CPS are critical to national efforts to reduce energy use while increasing performance, reliability, and efficiency across economic sectors—via the smart grid, smart transportation systems, smart manufacturing, and smart buildings infrastructure.

CPS is already facilitating a broad shift from hospital-based to home-based health care and expanding independent living opportunities for seniors. By extending the reach of quality care beyond traditional hospitals, CPS-based medical devices and systems are enabling more individualized health care and improved patient outcomes. As advances are made, CPS can lead to new capabilities to diagnose, treat, and prevent disease.

In national defense, CPS now delivers superiority in virtually all weapons systems, including manned and unmanned aircraft, ground vehicles, robotic platforms, surface and underwater vessels, and the overarching systems that integrate the nation’s fighting forces. In homeland security and law enforcement, CPS is used in diverse roles from bomb disposal and emergency response robotics to sensor networks providing advance warning of catastrophic events.

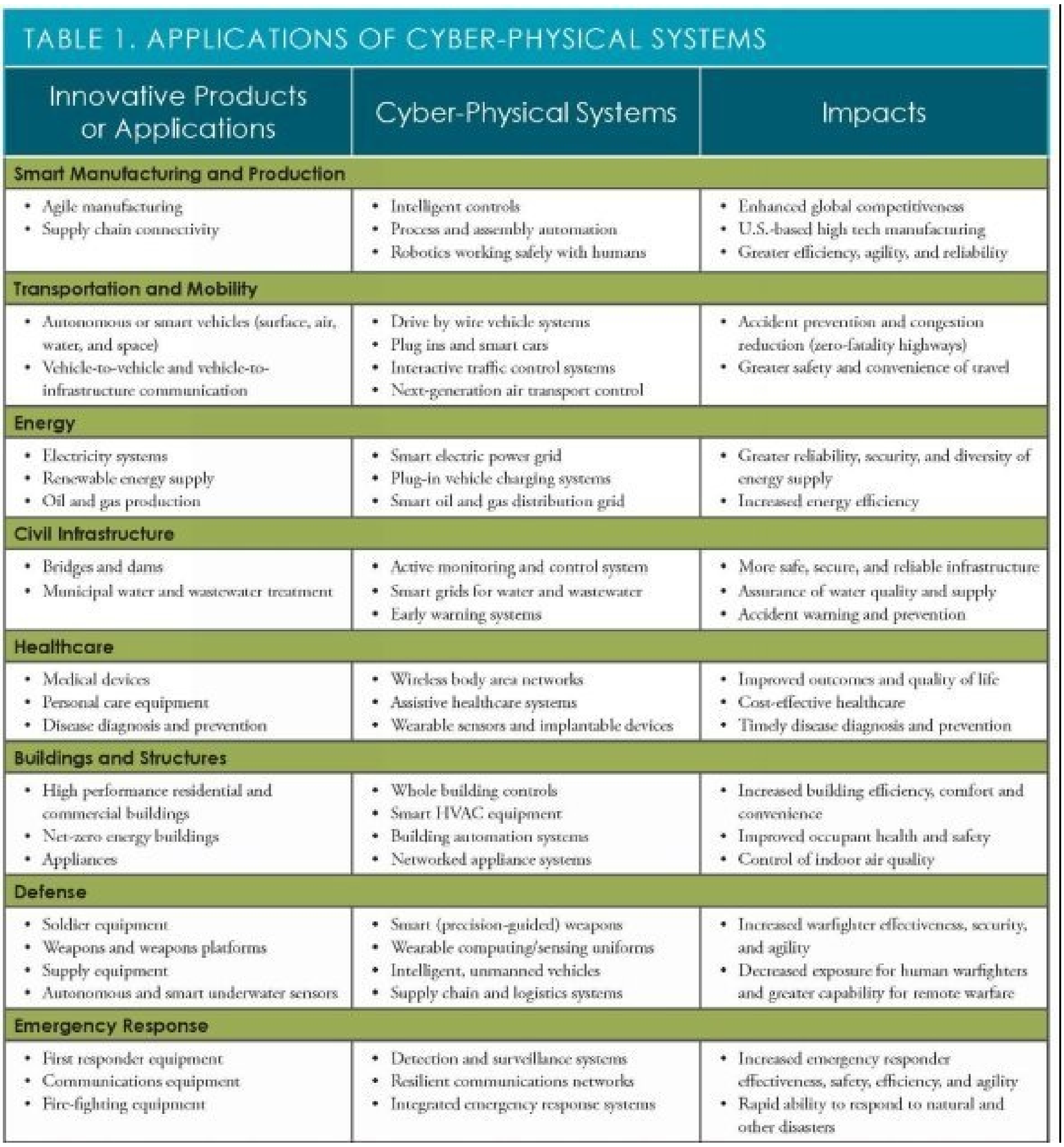
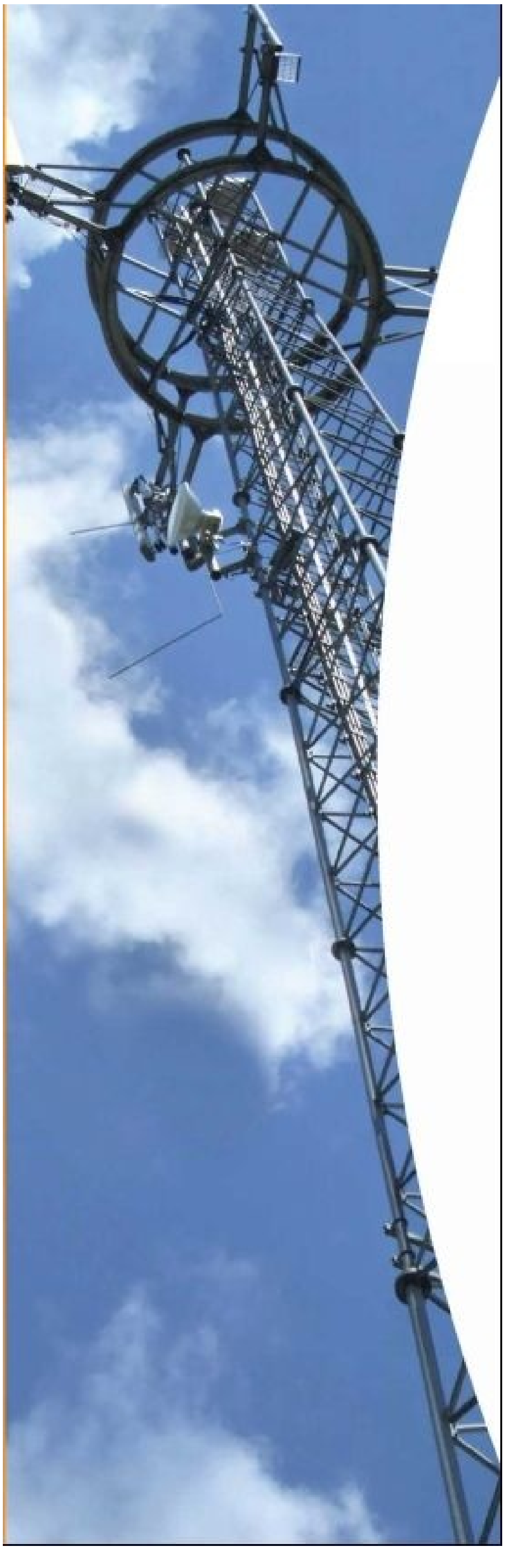


TABLE 1. APPLICATIONS OF CYBER-PHYSICAL SYSTEMS

Innovative Products or Applications	Cyber-Physical Systems	Impacts
Smart Manufacturing and Production		
• Agile manufacturing • Supply chain connectivity	• Intelligent controls • Process and assembly automation • Robotics working safely with humans	• Enhanced global competitiveness • U.S.-based high tech manufacturing • Greater efficiency, agility, and reliability
Transportation and Mobility		
• Autonomous or smart vehicles (surface, air, water, and space) • Vehicle-to-vehicle and vehicle-to-infrastructure communication	• Drive by wire vehicle systems • Plug ins and smart cars • Interactive traffic control systems • Next-generation air transport control	• Accident prevention and congestion reduction (zero-fatality highways) • Greater safety and convenience of travel
Energy		
• Electricity systems • Renewable energy supply • Oil and gas production	• Smart electric power grid • Plug-in vehicle charging systems • Smart oil and gas distribution grid	• Greater reliability, security, and diversity of energy supply • Increased energy efficiency
Civil Infrastructure		
• Bridges and dams • Municipal water and wastewater treatment	• Active monitoring and control system • Smart grids for water and wastewater • Early warning systems	• More safe, secure, and reliable infrastructure • Assurance of water quality and supply • Accident warning and prevention
Healthcare		
• Medical devices • Personal care equipment • Disease diagnosis and prevention	• Wireless body area networks • Assistive healthcare systems • Wearable sensors and implantable devices	• Improved outcomes and quality of life • Cost-effective healthcare • Timely disease diagnosis and prevention
Buildings and Structures		
• High performance residential and commercial buildings • Net-zero energy buildings • Appliances	• Whole building controls • Smart HVAC equipment • Building automation systems • Networked appliance systems	• Increased building efficiency, comfort and convenience • Improved occupant health and safety • Control of indoor air quality
Defense		
• Soldier equipment • Weapons and weapons platforms • Supply equipment • Autonomous and smart underwater sensors	• Smart (precision-guided) weapons • Wearable computing/sensing uniforms • Intelligent, unmanned vehicles • Supply chain and logistics systems	• Increased warfighter effectiveness, security, and agility • Decreased exposure for human warfighters and greater capability for remote warfare
Emergency Response		
• First responder equipment • Communications equipment • Fire-fighting equipment	• Detection and surveillance systems • Resilient communications networks • Integrated emergency response systems	• Increased emergency responder effectiveness, safety, efficiency, and agility • Rapid ability to respond to natural and other disasters



BROAD CHALLENGES FOR CYBER-PHYSICAL SYSTEMS

The interconnection of networking, computing, physical, and human components reaches most engineered systems and yields revolutionary new capabilities. The underlying technical challenges also have a great deal of commonality reflecting a range of fundamental scientific, engineering, institutional, and societal issues. Barriers arise throughout all stages of technology development, from basic science through applied R&D, demonstration, manufacturing, and deployment. Addressing the most critical of these will help ensure that in the future CPS are reliable, safe, producible, and secure.

SCIENTIFIC AND TECHNICAL CHALLENGES

Advancement in CPS requires a new systems science that encompasses both physical and computational aspects. Systems and computer science has provided a solid foundation for spectacular progress in engineering and information technology; a type of new systems science is now needed to address the unique scientific and technical challenges of CPS.

Integrating complex, heterogeneous large-scale systems. Future CPS will contain heterogeneous distributed components and systems of large numbers that must work together effectively to deliver expected performance. There are several challenges to achieving this today. A fundamental issue is the lack of common terminology, modeling languages, and rigorous semantics for describing interactions—physical and computational—across heterogeneous systems. Achieving the interoperability and compositionality of various components constructed in different engineering domains and sectors, without the benefit of unifying theories and standards, presents a major challenge. A lack of clear ownership of the interface between systems (e.g., between code, hardware, and multiple equipment vendors) also contributes to interoperability and integration problems. in addition to standards, interoperable systems need to ensure that timely outputs, outcome agreements, resilience, data transfers, and technical security protocols are addressed seamlessly within and between components. This includes aggregating and sharing data within systems as well as across systems and components.

Interaction between humans and systems. Current models for human and machine behaviors are not adequate for designing CPS when humans and machines closely interact. One of the challenges is modeling and measuring situational awareness—human perception of the system and its environment and changes in parameters that are critical to decision-making. This is particularly necessary for complex, dynamic systems, such as those used in aviation, air traffic control, power plant operations, military command and control, and emergency services. in such systems situational awareness can involve large and unpredictable combinations of human and machine behavior. inadequate situational awareness and limited ability to model the human component in large complex systems has been identified as one of the primary factors in accidents related to human error (Nullmeyer et al, 2005).

Dealing with uncertainty. Complex CPS need to be able to evolve and operate reliably in new and uncertain environments. An increasing number of these systems will also demonstrate emergent and unknown behaviors as they become more and more reliant on machine learning methodologies. in both cases, uncertainty in the knowledge or outcome of a process will require new ways to quantify uncertainty during the CPS design and development stages. Current methods for characterization and quantification of uncertainty are limited and inadequate. This is exacerbated by the limits of reliability and accuracy of physical components, the validity of models characterizing them, network connections, and potential design errors in software. Ongoing debate also surrounds the expectations for quantifying uncertainty, that is, attaining perfect results given the uncertainty of the physical world and approximations in design.

Measuring and verifying system performance. The difficulty of verifying performance, accuracy, reliability, security, and various other requirements impedes development and investment in CPS. Today’s capabilities for verification and validation (V&V) of CPS are limited, time consuming, and costly, particularly when compared to development time. Two major challenges are the creation of methodologies to further the capabilities of V&V of complex systems, and the development of test beds and datasets to support a principled approach to the validation of complex CPS. if the design phase is more reliable, testing can become more informed and require less time. The evaluation challenges will become increasingly difficult at the larger scales and higher complexity expected for future CPS, which will have massive and interconnected sensor, actuator, and component networks.

Robots can be designed to accomplish tasks that were not possible before. At left, researchers at the National Renewable Energy laboratory are using new robots to fabricate and analyze thin-film solar photovoltaic cells with greater precision and speed than ever before possible. When working with silicon, the robot can build a semi-conductor on a six-inch-square plate in about 35 minutes—while analyzing anomalies and light absorption and preparing the next plates. The robot is able to complete tasks that previously required as many as five laboratories.

Credit: NREL 17161/Pat Corkery (NREL, 2010)

Metrics are essential for the evaluation of many aspects of CPS, from design to testing, deployment, and operation. Key areas where scientifically-based metrics are needed include complexity, adaptability, safety, security, privacy, resilience, reliability, and manufacturability. One major challenge is to design metrics with sufficient flexibility to be applicable to a wide variety of systems. Determining how to use metrics effectively presents another challenge. For example, if metrics for privacy are defined, then design methods for achieving privacy objectives must also be developed. There are also challenges in modeling privacy requirements so that a system can be validated against these requirements.

System design. The design of CPS is hampered by the limited ability to design at a systems-level. There are many factors impeding system-level design, such as the lack of formalized high fidelity models for large systems, insufficient ways of measuring performance, and inadequate scientific foundations (e.g., no ‘science of systems’). A key factor is compositionality 1 and modularity in the design approach. Compositionality in CPS is impacted by the strong interdependencies of software and systems engineering and often limited by poor system design. For example, CPS development could be greatly facilitated if system components could be developed and verified in isolation and the system-level properties inferred from the properties of its parts. Designers of CPS aspire to this modular and compositional approach both in design and verification. However, it is only currently possible in narrow domains and with restricted, simple properties. Scientific and technical challenges to achieving compositionality include a lack of mathematical and system science foundations, formalized metrics, evaluation techniques, and methods for dealing with cross-cutting properties in the design space. Furthering the mathematical methodology for design space exploration is critical for allowing a principled approach to design complex architectures that are modular.

1 Compositionality in this sense means that system-level properties or performance can be derived from the local properties of individual components.

INSTITUTIONAL, SOCIETAL, AND OTHER CHALLENGES

Trust, security, and privacy.

Assuring that systems are trustworthy, secure, and protect the privacy of information creates both technical and policy challenges. Cyber-security is a critical aspect of CPS on many levels, including the protection of national infrastructure, privacy of individuals, system integrity, and intellectual property. Recent foreign-based intrusions on U.S. computer systems, both government and commercial, illustrate the current vulnerabilities of the Internet and the rationale for addressing the global security of cyberspace (GAO, 2010). While cyber-security is a strong national priority and much progress has been made to ensure protection from cyber-attacks, CPS security raises a host of new challenges. For example, the combination of cyber and physical vulnerabilities may lead to attack models that are fundamentally new, hard to analyze, and carry substantial risk in maintaining physical integrity of critical systems.

Challenges to secure CPS include modeling the security threat, developing a formal approach to CPS vulnerability assessments, and designing evolutionary and resilient architectures to handle rapidly evolving cyber and physical threats. Along with security, maintaining privacy and confidentiality is an important aspect. patients depending on implanted medical devices, for example, want protection of their identity and critical health information that could be exposed via the connection of their devices to monitoring networks. Industry requires protection of intellectual property as well as sensitive business and demographic information. Assuring the confidentiality of information and controlling the access and use of data are challenging, especially as the systems that collect, manage, and analyze information are rapidly evolving and in some cases need to operate in a distributed or relatively open environment.

Effective models of governance. The rapidly emerging global networks of CPS in energy, air traffic, transportation, cloud-based services and many others call for new governance models—both domestic and global—for providing standards, protocols, and oversight of systems that operate both in physical and cyber space. These new governance models are being explored but are not yet formalized. Governance could provide structured control and regulation for these systems and reduce liabilities that arise because of unwanted intrusions or other vulnerabilities. Governance is being discussed in many organizations, ranging from expert forums to treaty-based, decision-making bodies within governments. There is growing debate around these issues, with some pushing for increased intergovernmental oversight while others contend that the private sector can self-regulate via development of appropriate economic incentives, rules, and controls.

Many factories have robots as well as humans working in them; but the two do not always work well together. At the Massachusetts Institute of Technology (MIT), researchers have come up with an algorithm that may make it easier and safer for humans and robots to work side-by-side, giving robots the tools to learn the preferences of a human coworker.

(MIT, 2012)

Creation of CPS business models. The extreme systems integration inherent in CPS is a disruptive technology that changes the status quo, creates new industries, and eliminates others. Transformation of traditional industries into those that are CPS-based is a complex, high risk process because it requires fusing the business models of the IT industry with those of engineering-based industries. These fused business models are not yet well-established and can be difficult to convey. A contributing factor is that economic and other data that could be used to support a business case are not well documented for CPS. The lack of a generic, proven business model can inhibit investments in new technologies and systems, in spite of the benefits.

Today's examples of successful CPS business models include the aviation industry, which has incorporated cyber-physical avionic systems in modern airplanes. In this case, the industry understands the safety implications and has developed stringent safety standards and certification processes. As CPS become larger and more complex, the issues of business risk and liability also increase. There is an opportunity to mitigate this risk by sharing the cost of developing precompetitive and infrastructure technologies.

Understanding the value of CPS. CPS will benefit from well-developed infrastructure, which requires significant upfront investment. The value of CPS needs to be better understood for such investments to occur. R&D on CPS is often described in terms that are theoretical or include vocabulary that is not readily recognized. As a result, understanding the substance and applying the results of CPS R&D can be challenging for businesses, decision-makers, and end-users. Less academic and more strategically insightful ways of presenting CPS research, benefits, and risks would facilitate quicker and less expensive industry adoption of emerging technologies as well as improved understanding of the benefits and applications of CPS research. Some studies have presented methods to successfully articulate the value of CPS-related technology (BAH, 2010) but overall this remains a challenge.

Multi-disciplinary education and collaboration. The science and engineering of CPS are cross-disciplinary in nature, requiring expertise in computer science, mathematics, statistics, engineering, and the full spectrum of physical sciences—even extending into the arts such as ethics and psychology. Working across disciplines can be challenging, as it requires experts with highly diverse backgrounds to communicate on a common basis. In academia, there is a lack of concentrated, multi-disciplinary CPS education and research, as efforts have focused on the cyber or physical domains rather than a combination of the two. Significant challenges exist in creating multi-disciplinary CPS programs within the existing university structure, which has historically been divided into conventional disciplines (e.g., computer science, engineering, chemistry). Academia has previously confronted and successfully addressed similar challenges, resulting in the creation of new, vibrant industries such as bio-engineering.

Skilled workforce. CPS are sophisticated, advanced technology systems that require knowledge and training to design, develop, implement, and use. They require new skills and a new workforce. Creating and maintaining a skilled workforce to support future CPS is a significant challenge in its own right. CPS technology is a rapidly changing field and mechanisms for training and continuing education will be needed, as well as qualified instructors that stay abreast of emerging developments. Rigorous tools for workforce training in CPS are not currently available but could be highly effective in creating and maintaining a future workforce.

Research programs in CPS across the nation are leading to new discoveries and technologies while helping to educate a multi-disciplinary future workforce. A considerable portion of this research is conducted through U.S. government programs.

For example, at the National Science Foundation (NSF) the CPS program provides support to universities to develop the core system science needed to engineer complex cyber-physical systems and fosters a research community committed to advancing research and education in CPS. At the Defense Advanced Research Projects Agency (DARPA), research is ongoing in several areas that will accelerate progress in CPS. These include adaptive vehicles, construction of high-assurance cyber-physical systems, and advanced model-based design methods for cyber-physical systems. Within agencies, research in CPS is underway on mission-oriented applications, such as the smart grid, intelligent buildings, and advanced medical devices. The activities in CPS across federal agencies are coordinated by the Networking and Information Technology R&D (NITRD) Senior Steering Group on CPS and the High Confidence Software and Systems Coordinating Group. This group fosters close communication and liaison among agencies, academia, and industry to address CPS R&D needs and facilitate interagency program planning in this field.

STRATEGIC R&D OPPORTUNITIES

A number of strategic R&D opportunities have been identified as critical to accelerating progress in CPS and overcoming some of the important challenges. These are illustrated in Table 2 and described in depth on the following pages. They cover the full spectrum of CPS design, development, implementation, and use, including:

- Science and engineering foundations
- System performance, quality, and acceptance
- Applied development and deployment
- Workforce for continuing innovation in CPS

Measurement science and technology advances are woven throughout these opportunities and impact all stages of CPS development, from fundamental science and discovery to commercialization and deployment. For example, the major challenges of interoperability, interactions between humans and machines, understanding uncertainty, and evaluating performance all have strong roots in measurement science and technology.

The strategic R&D opportunities are recurring themes that appear in multiple technology areas and consequently would have far-reaching impact if addressed. They represent the priority research that has been identified as essential to advancing the state of CPS and reaping the potential benefits to society and the nation.

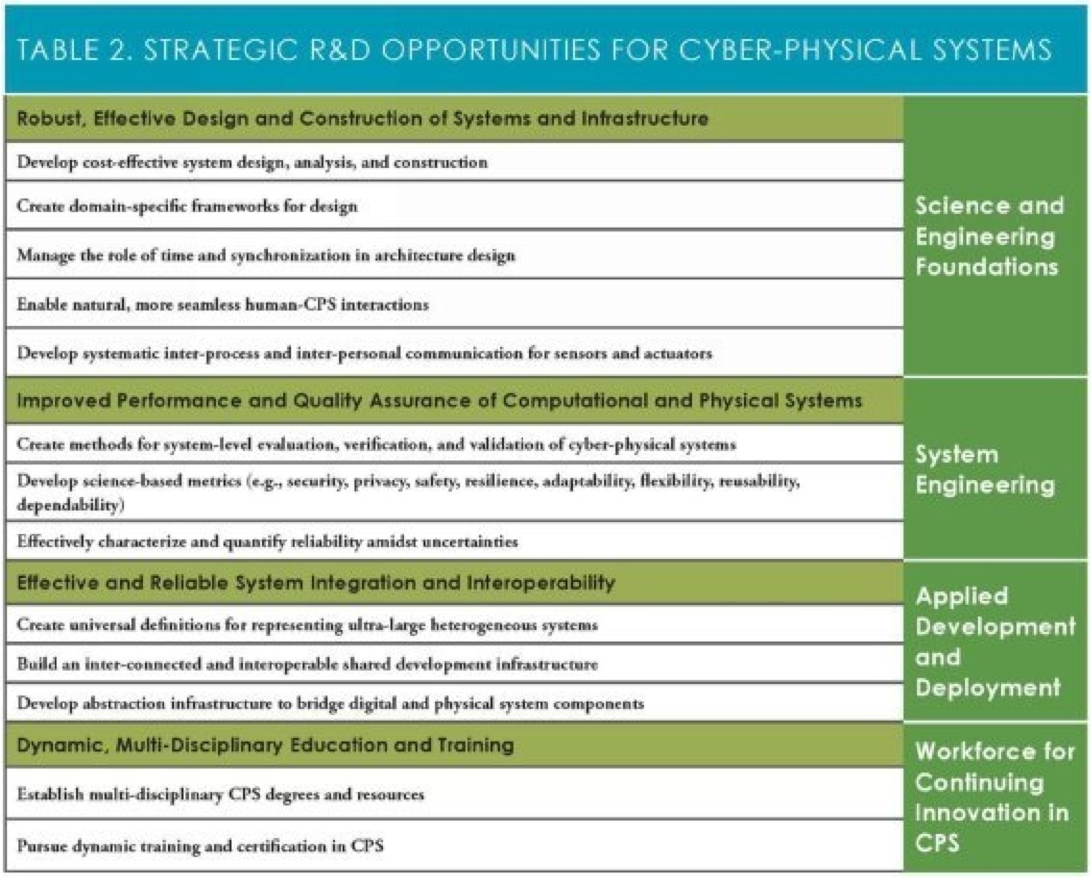


TABLE 2. STRATEGIC R&D OPPORTUNITIES FOR CYBER-PHYSICAL SYSTEMS

Robust, Effective Design and Construction of Systems and Infrastructure	**Science and Engineering Foundations**
Develop cost-effective system design, analysis, and construction	
Create domain-specific frameworks for design	
Manage the role of time and synchronization in architecture design	
Enable natural, more seamless human-CPS interactions	
Develop systematic inter-process and inter-personal communication for sensors and actuators	
Improved Performance and Quality Assurance of Computational and Physical Systems	**System Engineering**
Create methods for system-level evaluation, verification, and validation of cyber-physical systems	
Develop science-based metrics (e.g., security, privacy, safety, resilience, adaptability, flexibility, reusability, dependability)	
Effectively characterize and quantify reliability amidst uncertainties	
Effective and Reliable System Integration and Interoperability	**Applied Development and Deployment**
Create universal definitions for representing ultra-large heterogeneous systems	
Build an inter-connected and interoperable shared development infrastructure	
Develop abstraction infrastructure to bridge digital and physical system components	
Dynamic, Multi-Disciplinary Education and Training	**Workforce for Continuing Innovation in CPS**
Establish multi-disciplinary CPS degrees and resources	
Pursue dynamic training and certification in CPS	

123.775
112.30
LYBE / LYPG
LYBE
LYPG

SCIENCE AND ENGINEERING FOUNDATIONS

Opportunity

Robust, effective design and construction of systems and infrastructure

The development of CPS requires a new systems science foundation that can effectively integrate the elements of complex computational systems and processes with physical systems. Building blocks for design involve modeling, synthesis, simulation, and verification capabilities, new design tools and frameworks, ontologies and modeling *languages that cross discipline boundaries, methods that enable scalability from concept to operation, and the means to ensure a range of functional, performance, safety, security, and reliability requirements.*

Develop cost-effective system design, analysis, and construction methods - Before making large investments in a prototype CPS, it is important for designers to create a model to understand the dynamics of the many subsystems and their interactions, including the environment in which the deployed system must operate. Approaches are needed to develop models that are robust, semantically precise, reduce design and verification costs, and are reusable assets.

Today, building formalized, high fidelity models using mathematically based, formalized modeling languages is expensive, time consuming, and lacking tools and methods for large heterogeneous systems such as CPS. Such models should include an appropriate level of abstraction for the properties relevant to the system being designed, and be able to simulate system behavior under a range of conditions and assumptions. New, formal modeling methods are needed to create robust, physically relevant simulations that accurately recreate scenarios that CPS systems will experience in operation.

Creating more detailed models based on first principles is desirable but increases the number of parameters that must be estimated for model calibration—and the measurements required to fit these parameters can be difficult to obtain. Methods will be needed to recognize dominant parameters and apply abstractions to remove those that are less relevant from the model. For CPS this is especially important in developing models that are useful for studies at the systems level. Such models would evidence the phenomenological behaviors that emerge from the detailed first principles but balance abstraction and approximation, while characterizing these in light of the purpose they serve in system design.

The development and broad application of rigorous modeling tools could reduce the cost and duration of the design process, while improving design quality, performance, resilience, and dependability. Ultimately, domain-specific CPS design tools are required for aerospace, defense, transportation, medicine, and other industries that are built on standardized, configurable, and reusable tool suites for safety-critical and high-reliability systems.

In addition to system modeling, major challenges include designing to conflicting requirements of system components (which can cause unintended consequences), a lack of tools or framework for co-designing heterogeneous components and systems, a lack of design standards to enable interoperability, and a lack of foundations to enable compositionality. Co-design is a particularly critical factor in the development of systems that face extreme demands and require high levels of performance, safety and reliability. Interoperability is a challenge that is exacerbated in CPS where there are large, complex, highly networked systems and components originating from multiple domains and disciplines.

Create domain-specific frameworks for design — Engineering methods for co-design and new standards are needed that offer a common semantic foundation for modeling languages for exchange and translation across domains. Creating domain-specific design frameworks that are built on generic but customizable methods and tools would contribute substantially to reducing time to market, development costs, and the complexity of the design process. Finally, the design and implementation of CPS needs to be understood as a process that includes not only evaluation and co-design, but incorporates the ability to build sophistication as the levels of need advance.

Manage the role of time and synchronization in architecture design — Management of time and synchronization is a complex yet critical issue for real-time CPS. Generally speaking, synchronization is the coordination of events that must occur to operate a system and the coordination of time between the cyber and physical dimensions of CPS. In computer science, for example, synchronization refers to the coordination of simultaneous threads or processes to complete a task. With a mobile device, synchronization occurs when the device communicates with applications on a personal computer or server (e.g., syncing or docking the device). For a vehicle system or manufacturing unit, time management occurs in reference to physical processes that have actual physical consequences. Today, timekeeping technologies such as Global Positioning System satellites and the Network Time Protocol provide realtime approximation of Coordinated Universal Time (world time standard) and are used for many synchronization applications.

Poor timing and synchronization can result in data loss, downtime, and performance failure. Major challenges include effective timing and synchronization of multiple tasks, developing a unified, common view of time, measuring time and time scales, and communicating time characteristics to system components or sensors. Overcoming these challenges could impact any data driven, real-time application. Simply put, effective time management will make it easier for applications to run in a time-correct manner. Tackling these challenges may require multi-layered architecture for time management.

Standards for Autonomous Vehicles

There is a growing acceptance of either partially or fully autonomous mobile equipment in the manufacturing area. However, in manufacturing facilities people and mobile equipment frequently move through the same cluttered and constantly-changing environment. Standards are essential to reduce the potential for injury and ensure a safe environment. The ability to control multiple autonomous vehicles from different manufacturers with different sensing capabilities is also a challenge.

Enable natural, more seamless human-CPS interactions — A better model of human strengths and weaknesses and the corresponding machine strengths and weaknesses is needed to create a more natural, seamless interaction between humans and CPS. Models that are adaptive, implementable at varying degrees of sophistication, and optimized for human interventions will help manage risks and safety as systems move toward mixed-initiative modes of operation. They could also make humans more comfortable with and accepting of machine interactions.

Cognitive models are needed for human-machine behavior that can be validated and become adaptable to interactions as they occur. Cognitive models should also consider the growing number of autonomous CPS and that human-machine interactions are increasingly participatory. The requirement to couple unpredictable human behavior with the predictable, hard-wired behavior of machines and physical systems creates inherent difficulties in developing such models.

Develop systematic inter-process and interpersonal communication for sensors and actuators — A core component of CPS is the interpretation of data from various sources. CPS can contain highly connected and massive networks of sensors, actuators, and other devices that collect and act on many types of data. It is inherently difficult to measure the behavior of complex systems that contain multiple pathways for data interpretation, planning, and control.

The need to measure human interactions adds another level of complexity and uncertainty. A structured design and process integration method is needed to systematically relate multiple signals and symbols for inter-process and interpersonal communications across domains and applications. This would enable the development of less expensive plug-and-play sensors, create opportunities for modular, plug-and-play CPS, and lead to structured design and integration tools that reduce the cost and time to market of new systems.

SYSTEM PERFORMANCE, QUALITY, AND ACCEPTANCE

Opportunity

improved performance and quality assurance of computational and physical systems

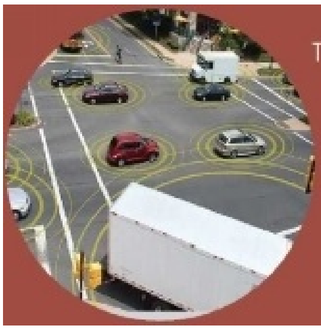
Development and acceptance of CPS in real-world applications will require assurances that these systems will perform as expected. Assessing both performance and quality involves V&V of the functioning of the entire system as well as individual components. The ability to infer the performance and quality of the entire system from its components can be advantageous—a property that is often referred to as compositionality—but is challenging to achieve in practice. The ability to compare performance and quality consistently across systems is essential but will require standardized, science-based metrics for safety, security, resilience, and other key parameters. Predicting operational performance and quality characteristics of CPS with high confidence (i.e., quantified assessment) is especially important for systems that operate autonomously or that directly impact human health and safety.

Create methods for system-level evaluation, verification, and validation of CPS — Evaluating the performance of CPS against system requirements is needed to facilitate acceptance, investment, and practical use of these systems. Some classes of CPS will require extensive and sustained investment (e.g., smart transportation, smart grid) and a solid understanding of potential performance to move technologies forward. System-level evaluation can be performed with V&V methods, especially for safety and trustworthiness requirements, but without standardized requirements, V&V is customized and costly. V&V is also challenged by an inability to effectively evaluate the whole system (how well components work in concert) since the performance of individual components (i.e., cyber, physical, and cyber-physical assemblies) does not necessarily translate to overall system performance. The difficulty of evaluating integrated components which interact in multiple temporal, spatial, and power scales also adds to the challenge. Cost effective methods of verifying and validating CPS could help decrease the cost of system integration, while increasing system reliability.

Foundations and infrastructure are currently lacking for evaluation and V&V of emerging CPS, but could be developed by leveraging methods and tools already in use in other systems. An integrated approach will be needed to enable greater understanding of the interactions between components, the role and impact of interfaces, and emerging system properties.

Autonomously operating systems (those with little human interaction or decision making) require certification processes that attest to assured system performance. Certification is a judgment that a system is adequately safe, secure, or meets other criteria for a given application in a set environment. To be valid, this judgment should be based on as much explicit and credible evidence as possible, with a foundation in good metrics including ways to measure complexity.

However, certification of complex, heterogeneous systems is extremely difficult, particularly in the design phase. Currently, system architecture, design, integration, and design space exploration are only robust enough to allow for building systems first, then testing and certifying. A challenge is to create methodology to enable compositional certification, which includes certification of components separately without the need for recertifying after the system components are integrated.



The U.S. Department of Transportation (DOT) is exploring use of short-range communication in "smart" cars to improve vehicle safety. Intersection-connected vehicles can improve safety at busy intersections.

Credit: U.S. Department of Transportation

Another challenge is integrating design artifacts and analyses as evidence (including partial and historic) into the certification process.

Develop science-based metrics for system qualities (e.g., security, privacy, safety, resilience, adaptability, flexibility, reusability, dependability) — A universal set of science-based metrics is needed to evaluate and predict how CPS will perform with respect to key system-level properties such as security, privacy, safety, resiliency, and dependability. Dependability in this case means that a system is highly reliable when running, but also capable of effectively predicting, recognizing, and quickly covering from unforeseen events. While it is technically challenging to develop scientifically-based measurements for these broad concepts, they are fundamental to developing and deploying dependable CPS.

Metrics are needed for all phases of CPS development, from the early design stages through prototype, testing, deployment, operation, and operation regimes (e.g., before and after system changes or failures). Design-phase metrics will enable engineers to build in safety, resilience, and dependability in the early stages of development. During the testing stage, metrics can help confirm that prototypes exhibit the desired characteristics. In deployment and operation, metrics can measure and monitor system behavior and provide indications of emerging issues. The use of science-based metrics will lead to greater system reliability and safety, and allow for fewer, lower-impact failures. Metrics could also be formulated to specify a minimum level of reliability and a maximum level of uncertainty. Metrics are also essential to supporting business models and investment because they will enable clear definition of questions of liability.

Effectively characterize and quantify reliability amidst uncertainties — Reliable CPS must behave with some degree of certainty, even in a dynamic, unpredictable environment. Characterization and quantification of reliability provides information on how a system responds to expected and unexpected events, and aids in understanding the potential risks to system operation. The numerous heterogeneous components, disparate characteristics of the physical versus cyber elements, and operational uncertainties found in CPS complicate the characterization of reliability. Failures could occur in both cyber and physical components and affect other system components in complex ways. For example, multiple car accidents experienced by a smart traffic control system could unexpectedly overload the information processing capacity and its ability to respond in real time.

Today, formal methods for determining reliability are lacking for most CPS and need to be developed. Such methods should be able to adapt to changing inputs, be able to compose disparate systems, and provide reproducible results. Effective characterization and quantification of reliability will ensure that systems are robust and resilient, and provide better understanding of potential risks to system operation.

SYSTEMS OF ENGINEERING

Opportunity

Effective and reliable system integration and interoperability

A unique characteristic of CPS is that they integrate computing and communication capabilities in the sensing and actuation functions of multiple components in the physical world. For CPS to operate dependably, safely, securely, efficiently, and in real time, some if not all components, whether cyber or physical, must be able to interact and communicate. These tightly coupled interactions require a high level of system integration and interoperability. System interfaces must be compatible and interactions should be governed by well-defined specifications; simulations of these interfaces should also use semantically precise modeling languages and vocabularies. In addition, individual components, as well as the total system, must be able to interact seamlessly with and respond to human operators and interventions.

Create universal definitions for representing ultra-large heterogeneous systems — Standard methods and shared conceptualization are needed for aligning the description of large, heterogeneous groups of system components, characteristic of many CPS, including specifications for technology, human elements, time, and space. Standard methods should include ways to universally and visually represent overall system behavior and performance of the integrated components. The objective of shared conceptualization is to provide standard definitions and/ or ways for readily translating or mapping between systems that can be embraced by both industry users and suppliers of technologies and subsystems. Developing agreements and methods to align CPS is complicated by the heterogeneity and disciplinary isolation of vocabularies and modeling languages for different aspects of large, heterogeneous systems. Challenges include an inability to measure the presence and correctness of complete system requirements and behavior of components within the context of the overall system. The key parameters that need to be universally defined must also be identified; this will require cross-disciplinary interactions among the cyber and physical sciences communities. If successfully developed, a consistent set of definitions could lower currently high integration and development costs, and provide a means to clarify top to bottom system behavior.

Computer scientists and engineers at Harvard University have created bug like ‘Kilobots’ that can interact and coordinate as a team, making it easier for researchers to test collective algorithms on hundreds or even thousands of tiny robots. In one demonstration 25 Kilobots displayed team- or swarm-like behaviors such as foraging, formation control, and synchronization. The robots are modeled after insects like ants and bees that participate in coordinated group behaviors such as food foraging, transporting large objects, and nest building. Support for this work was provided by the National Science Foundation and the Wyss Institute.

Build an inter-connected and interoperable shared development infrastructure — The current market does not have governance or business models in place to motivate the development of networked, cooperating, human interactive systems. Developers must assume the risk of sharing proprietary information with competitors and the liability of successfully integrating their systems with external systems to ensure high levels of performance and functionality. Building an infrastructure foundation that is interoperable, contains a balance of open source and proprietary information, and operates under the same standards will provide a protected framework from which interoperability issues are minimized and system development could be profitable. For example, the manufacturers of autonomous cars will have to work with each other as well as with the developers of the traffic regulating infrastructure to develop functional products. Building from a standard foundation would save time and cost through the sharing of critical information, while avoiding the liability of a solely proprietary product.

Develop abstraction infrastructure to bridge digital and physical system components — Innovative approaches to abstractions [2] and architectures that enable seamless integration of digital and physical systems for control, communication, and computation are needed for development of CPS. These need to support and facilitate cost-effective integration. Recently, computers and networks have pushed ahead into monitoring and controlling a variety of physical processes including feedback loops. In these systems, issues arise from the safety and reliability requirements of the physical components that are qualitatively different from those of the computing components. Because physical components are qualitatively different from software components, standard abstractions that are only physical or only computational fail when used in CPS.

For example, in communication networks, interfaces have been standardized between different layers of the network stack to allow heterogeneous systems to operate in

[2] In computer science, abstraction is the process of finding an alternate representation that embodies less detail but maintains the properties of interest of the original representation. As such, an abstraction is always relative to a set of properties.

a plug-and-play manner. This has created many opportunities for the proliferation of innovative technology and the Internet. However, today's science and engineering knowledge base does not include similar standardized abstraction layers and architectures to support integration and interoperability in CPS (Lee, 2012).

The objective is to develop a collaborative, open, and highly-evolvable abstraction framework and infrastructure that spans multiple domains and applications. The outcomes would be a greater confidence in the integration of cyber and physical components, the ability for system-wide and compositional evaluation, and greater openness of systems.

WORKFORCE FOR CONTINUING INNOVATION

Opportunity

Dynamic, multi-disciplinary education and training

Building and sustaining a workforce capable of developing, innovating, and operating future CPS will require significant enhancements in engineering curricula, renewed emphasis on systems sciences and engineering, and an increased emphasis on multidisciplinary research. Dynamic training programs for engineers, operators, and users of these systems will create pathways for keeping the workforce on top of new developments as they emerge.

Establish multi-department CPS degrees and resources — University systems have historically been divided into traditional disciplines (e.g., computer science, electrical engineering). To build and sustain a future workforce for CPS will require the incorporation of multi-disciplinary and targeted educational programs within the existing university structure. A prototype program could be developed in coordination with the National Academy of Engineering, the Accreditation Board for Engineering and Technology, and university organizations supporting research in CPS. Development of new textbooks and courses relevant to the curricula would need to occur in parallel. The objective is to create a more formal teaching and training approach in CPS leading to a new generation of scientists and engineers qualified and interested in working in this field. CPS educational programs will also appeal to students with an interest in new media by providing opportunities for gaining knowledge in emerging IT modalities.

Pursue dynamic training and certification in CPS — CPS is a dynamic field that requires continuous education and retraining. A number of approaches are possible, including development of CPS degrees, certifications, and accreditations, onsite training programs, or robust internships that allow for multi-disciplinary training. For example, a joint industrial and academic certification committee could be formed to develop a prototype test certification and accreditation for CPS training.

Twenty years ago, it took a week to purify a single protein. Today, robotic chromatography systems are making it possible to dramatically reduce the time needed for protein purification. Above, Irina Dementieva, a biochemist, and Youngchang Kim, a biophysicist and crystallographer, work with the first robot of its type in the U.S. to automate protein purification.

CONCLUSION

The potential of CPS to change every aspect of life is enormous. Concepts such as autonomous cars, robotic surgery, intelligent buildings, smart electric grid, smart manufacturing, and implanted medical devices are just some of the practical examples that have already emerged. These systems all rely on a computational core that is tightly conjoined and coordinated with components in the physical world.

As systems evolve they will shift the reliance on human decision making into new, more strategic aspects and will increasingly rely on operationalizing human knowledge through computational intelligence. This can yield many advantages, such as the computational core detecting and responding faster than humans, being more precise and less prone to fatigue than humanly possible, or expanding the capabilities of the system beyond the operator's skills. As we become more dependent on CPS, the challenge is to design systems that are dependable and reliable—systems we can trust our lives with.

This report is a call to action. Progress has been made, but there are many challenges ahead. Overcoming these challenges creates exciting opportunities to ensure that the U.S. is a technology leader in the field of CPS with a globally competitive edge. Significant challenges outlined in this call to action include:

- **Robust, effective design and construction of systems and infrastructure** — key to designing dependable systems from the ground up and reducing cost and time to market;

- **Improved performance and quality assurance** — essential for spurring future investment, acceptance, and use of innovative systems that promise to provide revolutionary improvements to conventional practice;

- **Effective and reliable system integration and interoperability** — required for highly connected and networked components to work together effectively as a total system; and

- **Dynamic, multi-disciplinary education and training** — will make possible sustained growth and innovation and spawn a new generation of entrepreneurs, as well as the next generation of cyber-physical systems.

REFERENCES

GAO, 2010. Protecting the Federal Government's Information Systems and the Nation's Cyber Critical Infrastructures. Government Accountability Office, 2010. Accessed 12/18/12. http://www.gao.gov/highrisk/risks/safety-security/government_information_systems.php

GE, 2012. Peter C. Evans and Marco Annunziata, Pushing the Boundaries of Minds and Machines. General Electric, November 2012. Accessed 12/18/12. http://www.ge.com/docs/chapters/Industrial Internet.pdf

Harvard, 2012. "Kilobots are leaving the nest: Swarm of tiny, collaborative robots will be made available to researchers, educators, and enthusiasts." November 21, 2011. Accessed 12/10/12. http://www.seas.harvard.edu/news-events/press-releases/kilobots-are-leaving-the-nest and NSF News: http://www.nsf.gov/news/news_summ.jsp?cntn_id=122415

Lee, 2012. Edward A. Lee, Cyber Physical Systems: Design Challenges, International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), May 6, 2008, Orlando, FL.

MIT, 2012. “Robotic assistants may adapt to humans in the factory: New algorithm allows robots and humans to work side by side.” June 2012. MIT News Office. Accessed 12/18/12. http://web.mit.edu/newsoffice/2012/robot-manufacturing-0612.html

NREL, 2010. “NREL’s New Robots Scrutinize Solar Cells.” March 22, 2010. National Renewable Energy Laboratory Newsroom. Accessed 11/15/12. http://www.nrel.gov/news/features/feature_detail.cfm/ feature id=1547

Nullmeyer et al, 2005. Nullmeyer, R.T., Stella, D., Montijo, G.A., & Harden, S.W., “Human factors in Air Force flight mishaps: Implications for change.” Proceedings of the 27th Annual Interservice/Industry Training, Simulation, and Education Conference (paper no. 2260), Arlington, VA, National Training Systems Association, 2005.

PCAST, 2012. Report to the President on Capturing Domestic Competitive Advantage in Advanced Manufacturing. President’s Council of Advisors on Science and Technology (PCAST), July 2012. Accessed 10/31/12. http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_amp_steering_commit

BAH, 2010. Systems-2020 Study, Final Report. Booz Allen Hamilton, 2010. Accessed 12/18/12. http://www.acq.osd.mil/se/docs/ BAH-Systems-2020-Report-Final.pdf

FOR MORE INFORMATION CONTACT:

Albert J. Wavering

Chief, Intelligent Systems Division

Engineering Laboratory

National Institute of Standards and Technology

301-975-3418

wavering@nist.gov

www.nist.gov/el/isd

NIST

National Institute of Standards and Technology

U.S. Department of Commerce

* * * * * * * * * * * *

2015 Worldwide Threat Assessment of the U.S. Intelligence Community

Senate Armed Services Committee

James R. Clapper

Director of National Intelligence

February 26, 2015

INTRODUCTION

Chairman McCain, Ranking Member Reed, Members of the Committee, thank you for the invitation to offer the United States Intelligence Community's 2015 assessment of threats to US national security. My statement reflects the collective insights of the Intelligence Community's extraordinary men and women, whom I am privileged and honored to lead. We in the Intelligence Community are committed every day to provide the nuanced, multidisciplinary intelligence that policymakers, warfighters, and domestic law enforcement personnel need to protect American lives and America's interests anywhere in the world. Information available as of February 13, 2015 was used in the preparation of this assessment.

* * * * * * * * * * * *

GLOBAL THREATS

Cyber * Counterintelligence * Terrorism * Weapons of Mass Destruction and Proliferation * Space and Counterspace * Transnational Organized Crime * Economics and Natural Resources * Human Security

REGIONAL THREATS

Middle East and North Africa * Iraq * Syria * Islamic State of Iraq and the Levant * Iran * Libya * Yemen * Lebanon * Egypt * Tunisia * Europe * Turkey * Key Partners * Russia and Eurasia * Russia * Ukraine, Moldova, and Belarus * The Caucasus and Central Asia * East Asia * China * North Korea * South Asia * Afghanistan * Pakistan * India * Sub-Saharan Africa * West Africa * Sudan * South Sudan * Nigeria * Somalia * Lord's Resistance Army * Central African Republic * The Sahel * Latin America and the Caribbean * Cuba * Central America * Venezuela * Haiti

* * * * * * * * * * * *

GLOBAL THREATS

CYBER

Strategic Assessment

Cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact. The ranges of cyber threat actors, methods of attack, targeted systems, and victims are also expanding. Overall, the unclassified information and communication technology (ICT) networks that support US Government, military, commercial, and social activities remain vulnerable to espionage and/or disruption. However, the likelihood of a catastrophic attack from any particular actor is remote at this time. Rather than a "Cyber Armageddon" scenario that debilitates the entire US infrastructure, we envision something different. We foresee an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security.

• A growing number of computer forensic studies by industry experts strongly suggest that several nations—including Iran and North Korea—have undertaker offensive cyber operations against private sector targets to support their economic and foreign policy objectives, at times concurrent with political crises.

Risk. Despite ever-improving network defenses, the diverse possibilities for remote hacking intrusions, supply chain operations to insert compromised hardware or software, and malevolent activities by human insiders will hold nearly all ICT systems at risk for years to come. In short, the cyber threat cannot be eliminated; rather, cyber risk must be managed. Moreover, the risk calculus employed by some private sector entities does not adequately account for foreign cyber threats or the systemic interdependencies between different critical infrastructure sectors.

Costs. During 2014, we saw an increase in the scale and scope of reporting on malevolent cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information (Pll) compromised, or remediation costs incurred by US victims. For example:

• After the 2012-13 distributed denial of service (DDOS) attacks on the US financial sector, JPMorgan Chase (JPMorgan) announced plans for annual cyber security expenditures of S250 million by the end of 2014. After the company suffered a hacking intrusion in 2014, JPMorgan's CEO said he would probably double JPMorgan's annual computer security budget within the next five years.

• The 2014 data breach at Home Depot exposed information from 56 million credit/debit cards and 53 million customer email addresses. Home Depot estimated :he cost of the breach to be $62 million.

• In 2014, unauthorized computer intrusions were detected on the networks of the Office of Personnel Management (OPM) as well as its contractors, US Investigations Services (USIS) and KeyPoint Government Solutions. The two contractors were involved in processing sensitive PI I related to national security clearances for Federal Government employees.

• In August 2014, the US company, Community Health Systems, informed the Securities and Exchange Commission that it believed hackers "originating from China" had stolen Pll on 4.5 million individuals.

Attribution. Although cyber operators can infiltrate or disrupt targeted ICT networks, most can no longer assume that their activities will remain undetected. Nor can they assume that if detected, they will be able to conceal their identities. Governmental and private sector security professionals have made significant advances in detecting and attributing cyber intrusions.

- In May 2014, the US Department of Justice indicted five officers from China's Peoples' Liberation Army on charges of hacking US companies.

- In December 2014, computer security experts reported that members of an Iranian organization were responsible for computer operations targeting US military, transportation, public utility, and other critical infrastructure networks.

Deterrence. Numerous actors remain undeterred from conducting economic cyber espionage or perpetrating cyber attacks. The absence of universally accepted and enforceable norms of behavior in cyberspace has contributed to this situation. The motivation to conduct cyber attacks and cyber espionage will probably remain strong because of the relative ease of these operations and the gains they bring to the perpetrators. The result is a cyber environment in which multiple actors continue to test their adversaries' technical capabilities, political resolve, and thresholds. The muted response by most victims to cyber attacks has created a permissive environment in which low-level attacks can be used as a coercive tool short of war, with relatively low risk of retaliation Additionally, even when a cyber attack can be attributed to a specific actor, the forensic attribution often requires a significant amount of time to complete. Long delays between the cyber attack and determination of attribution likewise reinforce a permissive environment.

Threat Actors

Politically motivated cyber attacks are now a growing reality, and foreign actors are reconnoitering and developing access to US critical infrastructure systems, which night be quickly exploited for disruption if an adversary's intent became hostile. In addition, those conducting cyber espionage are targeting US government, military, and commercial networks on a daily basis. These threats come from a range of actors, including: (1) nation states with highly sophisticated cyber programs (such as Russia or China), (2) nations with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea), (3) profit-motivated criminals, and (4) ideologically motivated hackers or extremists. Distinguishing between state and non-state actors within the same country is often difficult—especially when those varied actors actively collaborate, tacitly cooperate, condone criminal activity that only harms foreign victims, or utilize similar cyber tools.

Russia. Russia's Ministry of Defense is establishing its own cyber command, which—according to senior Russian military officials—will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems. Russia's armed forces are also establishing a specialized branch for computer network operations.

- Computer security studies assert that unspecified Russian cyber actors are developing means to access industrial control systems (ICS) remotely. These systems manage critical infrastructures such as electric power grids, urban mass-transit systems, air-traffic control, and oil and gas distribution networks. These unspecified Russian actors have successfully compromised the product supply chains of three ICS vendors so that customers download exploitative malware directly from the vendors' websites along with routine software updates, according to private sector cyber security experts.

China. Chinese economic espionage against US companies remains a significant issue. The "advanced persistent threat" activities continue despite detailed private sector reports, public indictments, and US demarches, according to a computer security study. China is an advanced cyber actor; however, Chinese hackers often use less sophisticated cyber tools to access targets. Improved cyber defenses would require hackers to use more sophisticated skills and make China's economic espionage more costly and difficult to conduct.

Iran. Iran very likely values its cyber program as one of many tools for carrying out asymmetric but proportional retaliation against political foes, as well as a sophisticated means of collecting intelligence. Iranian actors have been implicated in the 2012-13 DDOS attacks against US financial institutions and in the February 2014 cyber attack on the Las Vegas Sands casino company.

North Korea. North Korea is another state actor that uses its cyber capabilities for political objectives. The North Korean Government was responsible for the November 2014 cyber attack on Sony Pictures Entertainment (SPE), which stole corporate information and introduced hard drive erasing malware into the company's network infrastructure, according to the FBI. This attack coincided with the planned release of a SPE feature film satire that depicted the planned assassination of the North Korean president.

Terrorists. Terrorist groups will continue to experiment with hacking, which could serve as the foundation for developing more advanced capabilities. Terrorist sympathizers will probably conduct low-level cyber attacks on behalf of terrorist groups and attract attention of the media, which might exaggerate the capabilities and threat posed by these actors.

Integrity of Information

Most of the public discussion regarding cyber threats has focused on the confidentiality and availability of information; cyber espionage undermines confidentiality, whereas denial-of-service operations and data-deletion attacks undermine availability. In the future, however, */e might also see more cyber operations that will change or manipulate electronic information in order to compromise its integrity (i.e. accuracy and reliability) instead of deleting it or disrupting access to it. Decisionmaking by senior government officials (civilian and military), corporate executives, investors, or others will be impaired if they cannot trust the information they are receiving.

- Successful cyber operations targeting the integrity of information would need to overcome any institutionalized checks and balances designed to prevent the manipulation of data, for example, market monitoring and clearing functions in the financial sector.

COUNTERINTELLIGENCE

We assess that the leading state intelligence threats to US interests in 2015 will continue to be Russia and China, based on their capabilities, intent, and broad operational scopes. Other states in South Asia, the Near East, and East Asia will pose increasingly sophisticated local and regional intelligence threats to US interests. For example, Iran's intelligence and security services continue to view the United States as a primary threat and have stated publicly that they monitor and counter US activities in the region.

Penetrating the US national decisionmaking apparatus and Intelligence Community will remain primary objectives for foreign intelligence entities. Additionally, the targeting of national security information and proprietary information from US companies and research institutions dealing with defense, energy, finance, dual-use technology, and other areas will be a persistent threat to US interests.

Non-state entities, including transnational organized criminals and terrorists, will continue to employ human, technical, and cyber intelligence capabilities that present a significant counterintelligence challenge. Like state intelligence services, these non-state entities recruit sources and perform physical and technical surveillance to facilitate their illegal activities and avoid detection and capture.

The internationalization of critical US supply chains and service infrastructure, including for the ICT, civil infrastructure, and national security sectors, increases the potential for subversion. This threat includes individuals, small groups of “hacktivists,” commercial firms, and state intelligence services.

Trusted insiders who disclose sensitive US Government information without authorization will remain a significant threat in 2015. The technical sophistication and availability of information technology that can be used for nefarious purposes exacerbates this threat.

TERRORISM

Sunni violent extremists are gaining momentum and the number of Sunni violent extremist groups, members, and safe havens is greater than at any other point in history. These groups challenge local and regional governance and threaten US allies, partners, and interests. The threat to key US allies and partners will probably increase, but the extent of the increase will depend on the level of success that Sunni violent extremists achieve in seizing and holding territory whether or not attacks on local regimes and calls for retaliation against the West are accepted by their key audiences, and the durability of the US-led coalition in Iraq and Syria.

Sunni violent extremists have taken advantage of fragile or unstable Muslim-majority countries to make territorial advances, seen in Syria and Iraq, and will probably continue to do so. They also contribute to regime instability and internal conflict by engaging in high levels of violence. Most will be unable to seize and hold territory on a large scale, however, as long as local, regional, and international support and resources are available and dedicated to halting their progress. The increase in the number of Sunni violent extremist groups also will probably be balanced by a lack of cohesion and authoritative leadership. Although the January 2015 attacks against Charlie Hebdo in Paris is a reminder of the threat to the West, most groups place a higher priority on local concerns than on a tacking the so-called far enemy—the United States and the West—as advocated by core al- Qa’ida.

Differences in ideology and tactics will foster competition among some of these groups, particularly if a unifying figure or group does not emerge. In some cases, groups —even if hostile to each other— will ally against common enemies. For example, some Sunni violent extremists will probably gain support from like-minded insurgent or anti-regime groups or within disaffected or disenfranchised communities because they share the goal of radical regime change.

Although most homegrown violent extremists (HVEs) will probably continue to aspire to travel overseas, particularly to Syria and Iraq, they will probably remain the most likely Sunni violent extremist threat to the US homeland because of their immediate and direct access. Same might have been inspired by calls by the Islamic State of Iraq and the Levant (ISIL) in late September for individual jihadists in the West to retaliate for US-led airstrikes on ISIL. Attacks by lone actors are among the most difficult to warn about because they offer few or no signatures.

If ISIL were to substantially increase the priority it places on attacking the West rather than fighting to maintain and expand territorial control, then the group's access to radicalized Westerners who have fought in Syria and Iraq would provide a pool of operatives who potentially have access to the United States and other Western countries. Since the conflict began in 2011, more than 20,000 foreign fighters—at least 3,400 of whom are Westerners—have gone to Syria from more than 90 countries.

WEAPONS OF MASS DESTRUCTION AND PROLIFERATION

Nation-states' efforts to develop or acquire weapons of mass destruction (WMD), their delivery systems, or their underlying technologies constitute a major threat to the security of the United States, its deployed troops, and allies. Syrian regime use of chemical weapons against the opposition further demonstrates that the threat of WMD is real. The time when only a few states had access to the most dangerous technologies is past. Biological and chemical materials and technologies, almost always dual-use, move easily in the globalized economy, as do personnel with the scientific expertise to design and use them. The latest discoveries in the life sciences also diffuse rapidly around the globe.

Iran Preserving Nuclear Weapons Option

We continue to assess that Iran's overarching strategic goals of enhancing its security, prestige, and regional influence have led it to pursue capabilities to meet its civilian goals and give it the ability to build missile-deliverable nuclear weapons, if it chooses to do so. We do not know whether Iran will eventually decide to build nuclear weapons.

We also continue to assess that Iran does not face any insurmountable technical barriers to producing a nuclear weapon, making Iran's political will the central issue. However, Iranian implementation of the Joint Plan of Action (JPOA) has at least temporarily inhibited further progress in its uranium enrichment and plutonium production capabilities and effectively eliminated Iran's stockpile of 20 percent enriched uranium. The agreement has also enhanced the transparency of Iran's nuclear activities, mainly through improved International Atomic Energy Agency (IAEA) access and earlier warning of any effort to make material for nuclear weapons using its safeguarded facilities.

We judge that Tehran would choose ballistic missiles as its preferred method of delivering nuclear weapons, if it builds them. Iran's ballistic missiles are inherently capable of delivering WMD, and Tehran already has the largest inventory of ballistic missiles in the Middle East. Iran's progress on space launch vehicles—along with its desire to deter the United States and its allies—provides Tehran with the means and motivation to develop longer-range missiles, including intercontinental ballistic missiles (ICBMs).

North Korea Developing WMD-Applicable Capabilities

North Korea's nuclear weapons and missile programs pose a serious threat to the United States and to the security environment in East Asia. North Korea's export of ballistic missiles and associated materials to several countries, including Iran and Syria, and its assistance? to Syria's construction of a nuclear reactor, destroyed in 2007, illustrate its willingness to proliferate dangerous technologies.

In 2013, following North Korea's third nuclear test, Pyongyang announced its intention to "refurbish and restart" its nuclear facilities, to include the uranium enrichment facility at Yongbyon, and to restart its graphite-moderated plutonium production reactor that was shut down in 2007. We assess that North Korea has followed through on its announcement by expanding its Yongbyon enrichment facility and restarting the reactor.

North Korea has also expanded the size and sophistication of its ballistic missile forces, ranging from close-range ballistic missiles to ICBMs, while continuing to conduct test launches. In 2014, North Korea launched an unprecedented number of ballistic missiles.

Pyongyang is committed to developing a long-range, nuclear-armed missile that is capable of posing a direct threat to the United States and has publicly displayed its <N08 road-mobile ICBM twice. We assess that North Korea has already taken initial steps toward fielding this system, although the system has not been flight-tested.

Because of deficiencies in their conventional military forces, North Korean leaders are focused on developing missile and WMD capabilities, particularly building nuclear weapons. Although North Korean state media regularly carries official statements on North Korea's justification for building nuclear weapons and threatening to use them as a defensive or retaliatory measure, we do not know the details of Pyongyang's nuclear doctrine or employment concepts. We have long assessed that, in Pyongyang's view, its nuclear capabilities are intended for deterrence, international prestige, and coercive diplomacy.

China's Expanding Nuclear Forces

The People's Liberation Army's (PLA's) Second Artillery Force continues to modernize its nuclear missile force by adding more survivable road-mobile systems and enhancing its silo-based systems. This new generation of missiles is intended to ensure the viability of China's strategic deterrent by providing a second strike capability. In addition, the PLA Navy continues to develop the JL-2 submarine-launched ballistic missile (SLBM) and might produce additional JIN-class nuclear-powered ballistic missile submarines. The JIN-class submarines, armed with JL-2 SLBMs, will give the PLA Navy its first long-range, sea-based nuclear capability. We assess that the Navy will soon conduct its first nuclear deterrence patrols.

Russia's New Intermediate-Range Cruise Missile

Russia has developed a new cruise missile that the United States has declared to be in violation of the Intermediate-Range Nuclear Forces (INF) Treaty. In 2013, Sergei Ivanov, a senior Russian administration official, commented in an interview how the world had changed since the time the INF Treaty was signed 1987 and noted that Russia was "developing appropriate weapons systems" in light of the proliferation of intermediate- and shorter-range ballistic missile technologies around the world. Similarly, as far back as 2007, Ivanov publicly announced that Russia had tested a ground-launched cruise missile for its Iskander weapon system, whose range complied with the INF Treaty "for now." The development of a cruise missile that is inconsistent with INF, combined with these statements about INF, calls into question Russia's commitment to this treaty.

WMD Security in Syria

In June 2014, Syria's declared CW stockpile was removed for destruction by the international community. The most hazardous chemical agents were destroyed aboard the MV CAPE RAY as of August 2014. The United States and its allies continue to work closely with the Organization for the Prohibition of Chemical Weapons (OPCW) to verify the completeness and accuracy of Syria's Chemical Weapons Convention (CWC) declaration. We judge that Syria, despite signing the treaty, has used chemicals as a means of warfare since accession to the CWC in 2013. Furthermore, the OPCW continues to investigate allegations of chlorine use in Syria.

SPACE AND COUNTERSPACE

Threats to US space systems and services will increase during 2015 and beyond as potential adversaries pursue disruptive and destructive counterspace capabilities. Chinese and Russian military leaders understand the unique information advantages afforded by space systems and services and are developing capabilities to deny access in a conflict. Chinese military writings highlight the need to interfere with, damage, and destroy reconnaissance, navigation and communication satellites. China has satellite jamming capabilities and is pursuing antisatellite systems. In July 2014, China conducted a nondestructive antisatellite missile test. China conducted a previous destructive test of the system in 2007, which created long-lived space debris. Russia's 2010 Military Doctrine emphasizes space defense as a vital component of its national defense. Russian leaders openly assert that the Russian armed forces have antisatellite weapons and conduct antisatellite research. Russia has satellite jammers and is pursuing antisatellite systems.

TRANSNATIONAL ORGANIZED CRIME

Transnational Organized Crime (TOC) is a global, persistent threat to our communities at home and our interests abroad. Savvy, profit-driven criminal networks traffic in drugs, persons, wildlife, and weapons; corrode security and governance; undermine legitimate economic activity and the rule of law; cost economies important revenue; and undercut US development efforts.

Drug Trafficking

Drug trafficking will remain a major TOC threat to the United States. Mexico is the largest foreign producer of US-bound marijuana, methamphetamines, and heroin, and the conduit for the overwhelming majority of US-bound cocaine from South America. The drug trade also undermines US interests abroad, eroding stability in parts of Africa and Latin America; Afghanistan accounts for 80 percent of the world's opium production.

Weak Central American states will continue to be the primary transit area for the majority of US-bound cocaine. The Caribbean is becoming an increasingly important secondary transit area for US- and European-bound cocaine. In 2013, the world's capacity to produce heroin reached the second highest level in nearly 20 years, increasing the likelihood that the drug will remain accessible and inexpensive in consumer markets in the United States, where heroin-related deaths have surged since 2007. New psychoactive substances (NPS), including synthetic cannabinoids and synthetic cathinones, pose an emerging and rapidly growing global public health threat. Since 2009, US law enforcement officials have encountered more than 240 synthetic compounds. Worldwide, 348 new psychoactive substances had been identified, exceeding the number of 234 illicit substances under international controls.

Criminals Profiting from Global Instability

Transnational criminal organizations will continue to exploit opportunities in ongoing conflicts to destabilize societies, economies, and governance. Regional unrest, population displacements, endemic corruption, and political turmoil will provide openings that criminals will exploit for profit and to improve their standing relative to other power brokers.

Corruption

Corruption facilitates transnational organized crime and vice versa. Both phenomena exacerbate other threats to local, regional, and international security. Corruption exists at some level in all countries; however, the symbiotic relationship between government officials and TOC networks is particularly pernicious in some countries. One example is Russia, where the nexus among organized crime, state actors, and business blurs the distinction between state policy and private gain.

Human Trafficking

Human trafficking remains both a human rights concern and a challenge to international security. Trafficking in persons has become a lucrative source of revenue - estimated to produce tens of billions of dollars annually. Human traffickers leverage corrupt officials, porous borders, and lax enforcement to ply their illicit trade. This exploitation of human lives for profit continues to occur in every country in the world - undermining the rule of law and corroding legitimate institutions of government and commerce.

Wildlife Trafficking

Illicit trade in wildlife, timber, and marine resources endangers the environment, threatens rule of law and border security in fragile regions, and destabilizes communities that depend on wildlife for biodiversity and ecotourism. Increased demand for ivory and rhino horn in Asia has triggered unprecedented increases in poaching in Africa. Criminal elements, often in collusion with corrupt government officials or security forces, are involved in poaching and movement of ivory and rhino horn across Africa. Poaching presents significant security challenges for militaries and police forces in African nations, which often are outgunned by poachers and their allies. Illegal, unreported, and unregulated fishing threatens food security and the preservation of marine resources. It often occurs concurrently with forced labor in the fishing industry.

Theft of Cultural Properties, Artifacts, and Antiquities

Although the theft and trafficking of cultural heritage and art are traditions as old as the cultures they represent, transnational organized criminals are acquiring, transporting, and selling valuable cultural property and art more swiftly, easily, and stealthily. These criminals operate on a global scale without regard for laws, borders, nationalities or the significance of the treasures they smuggle.

ECONOMICS AND NATURAL RESOURCES

The global economy continues to adjust to and recover from the global financial crisis that began in 2008; economic growth since that period is lagging behind that of the previous decade. Resumption of sustained growth has been elusive for many of the world's largest economies, particularly in European countries and Japan. The prospect of diminished or forestalled recoveries in these developed economies as well as disappointing growth in key developing countries has contributed to a readjustment of energy and commodity markets.

Energy and Commodities

Energy prices experienced sharp declines during the second half of 2014. Diminishing global growth prospects, OPEC's decision to maintain its output levels, rapid increases in unconventional oil production in Canada and the United States, and the partial resumption of some previously sidelined output in Libya and elsewhere helped drive down prices by more than half since July, the first substantial decline since 2008-09. Lower-priced oil and gas will give a boost to the global economy, with benefits enjoyed by importers more than outweighing the costs to exporters.

Macroeconomic Stability

Extraordinary monetary policy or "quantitative easing" has helped revive growth in the United States since the global financial crisis. However, this recovery and the prospect of higher returns in the United States will probably continue to draw investment capital from the rest of the world, where weak growth has left interest rates depressed.

Global output improved slightly in 2014 but continued to lag the growth rates seen before 2008. Since 2008, the worldwide GDP growth rate has averaged about 3.2 percent, well below its 20-year, pre-GFC average of 3.9 percent. Looking ahead, prospects for slowing economic growth in Europe and China do not bode well for the global economic environment.

Economic growth has been inconsistent among developed and developing economies alike. Outside of the largest economies—the United States, the EU, and China—economic growth largely stagnated worldwide in 2014, slowing to 2.1 percent. As a result, the difference in growth rates of developing countries and developed countries continued to narrow—to 2.6 percentage points. This gap, smallest in more than a decade, underscores the continued weakness in emerging markets, whose previously much-higher average growth rates helped drive global growth.

HUMAN SECURITY

Critical Trends Converging

Several trends are converging that will probably increase the frequency of shocks to human security in 2015. Emerging infectious diseases and deficiencies in international state preparedness to address them remain a threat, exemplified by the epidemic spread of the Ebola virus in West Africa. Extremes in weather combined with public policies that affect food and water supplies will probably exacerbate humanitarian crises. Many states and international institutions will look to the United States in 2015 for leadership to address human security issues, particularly environment and global health, as well as those caused by poor or abusive governance.

Global trends in governance are negative and portend growing instability. Poor and abusive governance threatens the security and rights of individuals and civil society in many countries throughout the world. The overall risk for mass atrocities—driven in part by increasing social mobilization, violent conflict, and a diminishing quality of governance—is growing. Incidents of religious persecution also are on the rise. Legal restrictions on NGOs and the press, particularly those that expose government shortcomings or lobby for reforms, will probably continue.

Infectious Disease Continues To Threaten Human Security Worldwide

Infectious diseases are among the foremost health security threats. A more crowded and interconnected world is increasing the opportunities for human and animal diseases to emerge and spread globally. This has been demonstrated by the emergence of Ebola in West Africa on an unprecedented scale. In addition, military conflicts and displacement of populations with loss of basic infrastructure can lead to spread of disease. Climate change can also lead to changes in the distribution of vectors for diseases.

- The Ebola outbreak, which began in late 2013 in a remote area of Guinea, quickly spread into neighboring Liberia and Sierra Leone and then into dense urban transportation hubs, where it began spreading out of control. Gaps in disease surveillance and reporting, limited health care resources, and other factors contributed to the outpacing of the international community's response in West Africa. Isolated Ebola cases appeared outside of the most affected countries—notably in Spain and the United States—and the disease will almost certainly continue in 2015 to threaten regional economic stability, security, and governance.

- Antimicrobial drug resistance is increasingly threatening global health security. Seventy percent of known bacteria have acquired resistance to at least one antibiotic that is used to treat infections, threatening a return to the pre-antibiotic era. Multidrug-resistant tuberculosis has emerged in China, India, Russia, and elsewhere. During the next twenty years antimicrobial drug-resistant pathogens will probably continue to increase in number and geographic scope, worsening health outcomes, straining public health budgets, and harming US interests throughout the world.

- MERS, a novel virus from the same family as SARS, emerged in 2012 in Saudi Arabia. Isolated cases migrated to Southeast Asia, Europe, and the United States. Cases of highly pathogenic influenza are also continuing to appear in different regions of the world. HIV/AIDS and malaria, although trending downward, remain global health priorities. In 2013, 2.1 million people were newly infected with HIV and 584,000 were killed by malaria, according to the World Health Organization. Diarrheal diseases like cholera continue to take the lives of 800,000 children annually.

• The world’s population remains vulnerable to infectious diseases because anticipating which pathogen might spread from animals to humans or if a human virus will take a more virulent form is nearly impossible. For example, if a highly pathogenic avian influenza virus like H7N9 were to become easily transmissible among humans, the outcome could be far more disruptive than the great influenza pandemic of 1918. It could lead to global economic losses, the unseating of governments, and disturbance of geopolitical alliances.

Extreme Weather Exacerbating Risks to Global Food and Water Security

Extreme weather, climate change, and public policies that affect food and water supplies will probably create or exacerbate humanitarian crises and instability risks. Globally averaged surface temperature rose approximately 0.8 degrees Celsius (about 1.4 degrees Fahrenheit) from 1951 to 2014; 2014 was warmest on earth since recordkeeping began. This rise in temperature has probably caused an increase in the intensity and frequency of both heavy precipitation and prolonged heat waves and has changed the spread of certain diseases. This trend will probably continue. Demographic and development trends that concentrate people in cities—often along coasts—will compound and amplify the impact of extreme weather and climate change on populations. Countries whose key systems - food, water, energy, shelter, transportation, and medical - are resilient will be better able to avoid significant economic and human losses from extreme weather.

• Global food supplies will probably be adequate for 2015 but are becoming increasingly fragile in Africa, the Middle East, and South Asia. The risks of worsening food insecurity in regions of strategic importance to the United States will increase because of threats to local food availability, lower purchasing power, and counterproductive government policies. Price shocks will result if extreme weather or disease patterns significantly reduce food production in multiple areas of the world, especially in key exporting countries.

• Risks to freshwater supplies—due to shortages, poor quality, floods, and climate change—are growing. These problems hinder the ability of countries to produce food and generate energy, potentially undermining global food markets and hobbling economic growth. Combined with demographic and economic development pressures, such problems will particularly hinder the efforts of North Africa, the Middle East, and South Asia to cope with their water problems. Lack of adequate water might be a destabilizing factor in countries that lack the management mechanisms, financial resources, political will, or technical ability to solve their internal water problems.

• Some states are heavily dependent on river water controlled by upstream nations. When upstream water infrastructure development threatens downstream access to water, states might attempt to exert pressure on their neighbors to preserve their water interests. Such pressure might be applied in international forums and also includes pressing investors, nongovernmental organizations, and donor countries to support or halt water infrastructure projects. Some countries will almost certainly construct and support major water projects. Over the longer term, wealthier developing countries will also probably face increasing water-related social disruptions. Developing countries, however, are almost certainly capable of addressing water problems without risk of state failure. Terrorist organizations might also increasingly seek to control or degrade water infrastructure to gain revenue or influence populations.

Increase in Global Instability Risk

Global political instability risks will remain high in 2015 and beyond. Mass atrocities, sectarian or religious violence, and curtailed NGO activities will all continue to increase these risks. Declining economic conditions are contributing to risk of instability or internal conflict.

- Roughly half of the world’s countries not already experiencing or recovering from instability are in the “most risk” and “significant risk” categories for regime-threatening and violent instability through 2015.

- Overall international will and capability to prevent or mitigate mass atrocities will probably diminish in 2015 owing to reductions in government budgets and spending.

- In 2014, about two dozen countries increased restrictions on NGOs. Approximately another dozen also plan to do so in 2015, according to the International Center for Nonprofit Law.

REGIONAL THREATS

MIDDLE EAST AND NORTH AFRICA

Iraq

Over six months into the coalition campaign against the Islamic State of Iraq and the Levant (ISIL), the frontlines against the group in Iraq have largely stabilized; no side is able to muster the resources necessary to attain its territorial ambitions. The Iraqi Security Forces (ISF), Peshmerga, Shia militants, and a few tribal allies—bolstered by air and artillery strikes, weapons, and advice from the United States, Arab and Western allies, and Iran—have prevented ISIL from gaining large swaths of additional territory.

Sectarian conflict in mixed Shia-Sunni areas in and around Baghdad that can undermine progress against ISIL is growing. ISF and Shia militants are conducting a campaign of retribution killings and forced displacement of Sunni civilians in several areas contested by Sunni militants.

Since taking office, Prime Minister al-Abadi has taken steps to change the ethno-sectarian tone in Baghdad, including engaging Sunni tribal leaders and reaching a tentative oil agreement with the Kurdistan Regional Government. However, the ethnosectarian nature of security operations and persistent distrust among Iraqi leaders risk undermining Abadi’s nascent political progress.

Syria

The Syrian regime made consistent gains in 2014 in parts of western Syria that it considers key, retaking ground in eastern Damascus, Horns, and Latakia; it is close to surrounding Aleppo city. The regime will require years to reassert significant control over the country.

- The bulk of the opposition in the north is fighting on three fronts—against the regime, the al-Qa'ida-affiliated Nusrah Front, and ISIL. The opposition in the south has made steady gains in areas that the regime has not made a priority and where ISIL has only a limited presence.

The stability of Syria's neighbors is at risk due to the country's prolonged conflict, which will strain regional economies forced to absorb millions of refugees. The conflict will also encourage regional sectarianism and continue to incubate extremist groups that will use Syria as a launching pad for attacks across the Middle East.

- The Syrian conflict is also putting huge economic and resource strains on countries in the region primarily due to the nearly 4 million refugees fleeing the conflict. Most of the refugees have fled to neighboring states. More than 620,000 are in Jordan; almost 1.6 million are in Turkey; almost 1.2 million are in Lebanon; and more than 240,000 are in Iraq. These states have requested additional international support to manage the influx.

Islamic State of Iraq and the Levant

In an attempt to strengthen its self-declared caliphate, ISIL probably plans to conduct operations against regional allies, Western facilities, and personnel in the Middle East; it has already executed Western and Japanese hostages as well as a Jordanian Air Force pilot. ISIL leader Abu Bakr al-Baghdadi outlined the group's ambitious external goals, including the expansion of the caliphate into the Arabian Peninsula and North Africa and attacks against Western, regional, and Shia interests, according to a public statement in November 2014.

- In September 2014, ISIL publicly called on all Sunnis to retaliate for US-led airstrikes in Iraq and Syria, advocating the targeting of law enforcement and other government officials using any means available. Individuals from Europe and North America who have trained and fought with ISIL can return home and conduct attacks either on their own or on ISIL's behalf. The French citizen arrested in May 2014 for a shooting at a Jewish museum in Brussels had returned from fighting, probably with ISIL in Syria, and was wrapped in a flag with ISIL inscriptions when he was apprehended. We do not know whether he acted at ISIL's behest.

Iran

The Islamic Republic of Iran is an ongoing threat to US national interests because of its support to the Asad regime in Syria, promulgation of anti-Israeli policies, development of advanced military capabilities, and pursuit of its nuclear program. President Ruhani—a longstanding member of the regime establishment—will not depart from Iran's national security objectives of protecting the regime and enhancing Iranian influence abroad, even while attempting different approaches to achieve these goals. He requires Supreme Leader Khamenei's support to continue engagement with the West, moderate foreign policy, and ease social restrictions within Iran.

Iran possesses a substantial inventory of theater ballistic missiles capable of reaching as far as some areas of southeastern Europe. Tehran is developing increasingly sophisticated missiles and improving the range and accuracy of its other missile systems. Iran is also acquiring advanced naval and aerospace capabilities, including naval mines, small but capable submarines, coastal defense cruise missile batteries, attack craft, antiship missiles, and armed unmanned aerial vehicles.

In Iraq and Syria, Iran seeks to preserve friendly governments, protect Shia interests, defeat Sunni extremists, and marginalize US influence. The rise of ISIL has prompted Iran to devote more resources to blunting Sunni extremist advances that threaten Iran's regional allies and interests. Iran's security services have provided robust military support to Baghdad and Damascus, including arms, advisers, funding, and direct combat support. Both conflicts have allowed Iran to gain valuable on-the-ground experience in counterinsurgency operations. Iranian assistance; has been instrumental in expanding the capabilities of Shia militants in Iraq. The ISIL threat has also reduced Iraqi resistance to integrating those militants, with Iranian help, into the Iraqi Security Forces, but Iran has uneven control over these groups.

Despite Iran's intentions to dampen sectarianism, build responsive partners, and deescalate tensions with Saudi Arabia, Iranian leaders—particularly within the security services—are pursuing policies with negative secondary consequences for regional stability and potentially for Iran. Iran's actions to protect and empower Shia communities are fueling growing fears and sectarian responses.

Libya

We assess that Libya will remain volatile in 2015. Political polarization and broadening militia violence have pushed Libya into a civil war. Nearly four years since the evolution that toppled Qadhafi, rival governments have emerged, leaving the country with no clear legitimate political authority or credible security forces. Militias aligned with the rival governments continue to vie for dominance in Tripoli and Benghazi.

- In Benghazi, fighting that began in May 2014 is ongoing between forces aligned with former General Khalifa Hater's Operation Dignity forces and Ansar al-Sharia (AAS) and allied groups. In Tripoli, the Libya Dawn militias have driven their Zintani militia rivals out of the city, but fighting continues southwest of Tripoli.

- UN efforts to facilitate a negotiated resolution between Libya's rival governments have shown limited momentum but as of early February 2015 have not made tangible progress toward a unity government or a durable cease-fire.

Extremists and terrorists from al-Qa'ida-affiliated and allied groups are using Libya's permissive security environment as a safe haven to plot attacks, including against Western interests in Libya and the region. ISIL also has declared the country part of its caliphate, and ISIL-aligned extremists are trying to institute sharia in parts of the country.

Yemen

The Huthis have emerged as the most powerful group in Yemen since taking Sanaa last fall and are poised to dominate the political process after President's Hadi's resignation and their dissolution of the government. The group, however, continues to face resistance as it expands toward the south and east. Southern Yemeni leaders have been alarmed by the Huthi's consolidation of control in Sanaa and are poised to oppose further Huthi expansion south. Al-Qa'ida in the Arabian Peninsula (AQAP) has taken advantage of many Sunni tribes' opposition to Huthi expansion to gain recruits to fight against the Huthis.

Chronic and severe economic and humanitarian problems, exacerbated by repeated pipeline attacks and the Huthis' push to reinstate costly fuel subsidies, will continue to undercut government control and legitimacy. Yemen will probably continue pressuring donor nations to make good on aid pledges while negotiating with tribes outside of Sanaa's control to keep oil exports flowing.

Huthi ascendency in Yemen has increased Iran's influence as well.

Lebanon

Lebanon continues to struggle with spillover from the Syrian conflict, including periodic sectarian violence: terrorist attacks: and the economic, political, and sectarian strain associated with refugees.

- Lebanon faces growing threats from terrorist groups, including the al-Nusrah Front and ISIL. Sunni extremists are trying to establish networks in Lebanon and nave increased attacks against Lebanese army and Hizballah positions along the Lebanese-Syrian border. Lebanon potentially faces a protracted conflict in northern and eastern parts of the country from extremist groups seeking to seize Lebanese territory, supplies, and hostages.

- The presence of over one million mostly Sunni Syrian refugees in Lebanon, which has a population of only 4.1 million, has significantly altered Lebanon's sectarian demographics and is a continuing burden on the Lebanese economy. In October 2014, the cabinet further tightened entry restrictions to allow only "extreme humanitarian cases" into the country. Arrivals have declined 75 to 90 percent since August, most recently due in part to the new restrictions.

Egypt

Egyptian officials have announced that legislative elections will start in March 2015 and that voting will be staggered in phases over seven weeks. Egypt faces a persistent threat of terrorist and militant violence that is directed primarily at the state security forces both in the Sinai Peninsula and mainland Egypt. Since mid-2013, Sinai-based terrorist group Ansar Bayt al-Maqdis (ABM)—affiliated since November with ISIL—has claimed responsibility for some of the most sophisticated and deadly attacks against Egyptian security forces in decades.

Tunisia

Tunisia has transitioned to a permanent democratic government. Beji Caid Essebsi was elected President in the presidential runoff election in December 2014. In January 2015, Essebsi's political party Nidaa Tounes selected former Interior Minister Essid to become Prime Minister.

- In early February, Prime Minister Habib Essid formed a broad-based coalition government, led by Nidaa Tounes. which included Islamist party al-Nahda and several smaller parties. The new government almost certainly recognizes Tunisia's economic and security challenges.

The permanent government will inherit one of the highest youth unemployment rates in the world, a high budget deficit, and decreasing Foreign Direct Investment and balance of payments. It will struggle to meet public expectations for swift economic progress.

EUROPE

Turkey

Turkey will remain a critical partner in a wide range of US security policy priorities, including anti-ISIL and broader counterterrorism efforts. Joint US-Turkish efforts to stem instability in Iraq and Syria share the same goals but employ different approaches, increasing tension in the bilateral relationship. Turkish President Erdogan and leaders of the ruling Justice and Development Party (AKP) are focused on the general elections, which are scheduled to be held in June 2015

- Ankara will be more inclined to support the anti-ISIL coalition if the coalition agrees to focus efforts against Asad, including setting up an internationally guaranteed buffer zone in Syria.

- Turkey is concerned that the Kurdish Democratic Union (PYD)—a group it believes is affiliated with the Kurdistan People's Congress (KGK/former PKK)—will gain international legitimacy.

Key Partners

The Transatlantic partnership remains vital as the United State:, works with European leaders to maintain a concerted response to Russia's action in Ukraine and to other security challenges on the European continent and beyond. Europeans are working to address fiscal challenges and encourage economic growth while maintaining and strengthening financial governance.

- The Transatlantic Trade and Investment Partnership has the potential to help generate economic growth for both the United States and Europe, reinforce the transatlantic link, and address public concerns about data privacy and food and health standards.

RUSSIA AND EURASIA

Russia

The Ukrainian crisis has profoundly affected Russia's relations with the West and will have far-reaching effects on Russia's domestic politics, economic development, and foreign policy.

President Vladimir Putin enjoys some of his highest domestic approval ratings in all his years in office. An intense state media propaganda campaign has stoked Russians' perception that Putin righted a historical wrong in orchestrating Russia's seizure of Crimea and reasserted Russia's great-power interests against a hostile West.

At the same time, the crisis in Ukraine has exacerbated preexisting domestic problems in Russia. The fall of former Ukrainian President Viktor Yanukovych's government in February 2014 has almost certainly deepened the Kremlin's concerns over the dangers of mass demonstrations and has intensified the Kremlin's efforts to defuse what it sees as potential catalysts for protests in Russia.

Russia’s economy was in decline even before the crisis began. Growth stagnated in 2014 due to declining oil prices, large capital outflows, and a sharply declining ruble. In addition, economic sanctions cut off some Russian firms from Western financing. These factors have increased the real and perceived risks of doing business in Russia, raised the overall cost of international credit, and will probably drive Russia into recession in 2015.

Moscow is pushing for greater regional integration, pressing neighboring states to follow the example of Belarus and Kazakhstan and join the Moscow-led Eurasian Economic Union. The Kremlin is also cultivating its relationship with China, seeking to maintain some influence in Europe and emphasizing multilateral forums to counter what Moscow views as US unilateralism. These trends were already present in Russian diplomacy, but the Ukrainian crisis has almost certainly lent emphasis to these policies.

Russia is taking information warfare to a new level, working to fan anti-US and anti-Western sentiment both within Russia and globally. Russian state-controlled media publish false and misleading information in an effort to discredit the West, undercut consensus on Russia, and build sympathy for Russian positions.

In Ukraine, Russia has demonstrated its willingness to covertly use military and paramilitary forces in a neighboring state—a development that raises anxieties in states along Russia’s periphery. Future Russian deployments and force posture changes will probably be designed to maximize their diplomatic and public impact in Europe. Russian military officials have announced plans to conduct more “out-of-area” air and naval deployments, to include greater activity in the Caribbean and Mediterranean Seas.

Moscow has made headway in modernizing its nuclear and conventional forces, improving its training and joint operational proficiency, modernizing its military doctrine to integrate new methods of warfare, and developing long-range, precision-strike capabilities. Despite its economic difficulties, Moscow is committed to modernizing its military.

Ukraine, Moldova, and Belarus

Ukraine faces a daunting array of problems after nearly a year of conflict with Russia and its proxies in eastern Ukraine. At the same time, the crisis has fostered a sense of national identity and unity. Public opinion has shifted heavily in favor of pursuing integration with the EU while views of Russia have become sharply negative. Moreover, for the first time, a narrow majority of the population supports NATO membership.

Negotiations over the status of the separatist-held territory in eastern Ukraine will almost certainly be difficult and protracted. Russia has supplied substantial quantities of heavy weapons to strengthen the separatists’ forces and covertly supports them with its own troops, both within Ukraine and from across the border. More importantly, Moscow has demonstrated that it is willing to intervene directly to prevent the separatists from being defeated on the battlefield. Further fighting is likely in 2015.

Ukraine’s dire economic situation presents no less a challenge to Kyiv than the conflict in the east. Ukraine will be highly dependent on substantial outside financial assistance for years to come.

In Moldova, the narrow victory of pro-EU parties in the latest parliamentary elections suggests that Moldova will push ahead with its European integration agenda. However, Chisinau still faces numerous challenges in seeking to overcome economic difficulties, entrenched corruption, and Moscow's displeasure with Moldova's rejection of closer integration with Russia. Any progress on resolving the political status of the ethnic-Russian separatist region of Transnistria is unlikely.

On 1 January 2015, Belarus became, along with Kazakhstan, a founding member of the Eurasian Economic Union (EEU), a regional integration project that Moscow eventually plans to transform into a Eurasian Union as a counterpart to the EU. President Lukashenko has tread carefully in regard to the Ukrainian crisis, declining to recognize Russia's seizure of Crimea, but agreeing nevertheless to deepen military cooperation with Moscow.

The Caucasus and Central Asia

In Georgia, progress is unlikely on the core disputes between Tbilisi and Moscow, including Georgia's NATO aspirations and the status of the occupied territories of Abkhazia and South Ossetia. Tensions with Russia will remain high, and we assess that Moscow will press Tbilisi to abandon closer EU and NATO ties.

Armenia and Azerbaijan saw an increase in 2014 of ceasefire violations and a record number of casualties along the Line of Contact (LOC), which separates ethnic Armenian and Azerbaijani forces near the separatist region of Nagorno-Karabakh. The increased violence highlights how the close proximity of opposing military forces continues to pose a risk of miscalculation and unintended escalation. Prospects for a peaceful resolution in the foreseeable future are dim.

Central Asian states remain concerned about regional instability in light of a reduced Coalition presence in Afghanistan. Although they have long been alarmed about the activities of Central Asian militant groups operating in Afghanistan and Pakistan, they are increasingly worried about the threat posed by the return of the small but growing number of their nationals who have traveled to Syria to join violent Islamist extremist groups. On the whole, however, the Central Asian states will probably face more acute risks of instability in 2015 from internal issues such as unclear political succession plans, weak economies, ethnic tensions, and political repression—any of which could produce a crisis with little warning.

EAST ASIA

China

China will continue to pursue an active foreign policy—especially within the Asia Pacific—bolstered by increasing capabilities and its firm stance on East and South China Sea territorial disputes with rival claimants. The chances for sustained tensions will persist bees use competing claimants will probably pursue actions—including energy exploration—that others perceive as infringing on their sovereignty. China will probably seek to expand its economic role and outreach in the region, pursuing broader acceptance of its economic initiatives, including the Asia Infrastructure Investment Bank. Although China remains focused on regional issues, it will seek a greater voice on major international issues and in making new international rules.

Notwithstanding this external agenda, Chinese leaders will focus primarily on addressing domestic concerns. The Chinese Communist Party leadership under President Xi Jinping announced an ambitious agenda of legal reforms in late 2014 that built on its previous agenda of ambitious economic reforms—all aimed at improving government efficiency and accountability and strengthening the control of the Communist Party. The difficulty of implementing these reforms and bureaucratic resistance to them create the possibility of rising internal frictions as the agenda moves forward. Beijing will also remain concerned about the potential for domestic unrest or terrorist acts in Xinjiang and Tibet, which might lead to renewed human rights abuses. Following months of pro-democracy protests in late 2014, Chinese leaders will monitor closely political developments in Hong Kong for signs of instability.

North Korea

Three years after taking the helm of North Korea, Kim Jong Un has further solidified his position as unitary leader and final decision authority through purges, executions, and leadership shuffles. Kim was absent from public view for 40 days in late 2014, leading to widespread foreign media speculation about his health and the regime's stability. The focus on Kim's health's a reminder that the regime's stability might hinge on Kim's personal status. Kim has no clearly identified successor and is inclined to prevent the emergence of a clear "number two" who could consolidate power in his absence. Kim and the regime have publicly emphasized his focus on improving the country's troubled economy and the livelihood of the North Korean people while maintaining the tenets of a command economy. He has codified this approach via his dual-track policy of economic development and advancement of nuclear weapons. (Information on North Korea's nuclear weapons program and intentions can be found above in the section on WMD and Proliferation.) Despite renewed efforts at diplomatic outreach, Kim continues to challenge the international community with provocative and threatening behavior in pursuit of his goals, as prominently demonstrated in the November 2014 cyber attack on Sony.

SOUTH ASIA

Afghanistan

President Ashraf Ghani and Chief Executive Officer Abdullah Abdullah secured Parliament's approval of the Bilateral Security Agreement and NATO Status of Forces Agreement prior to the NATO Ministerial in December 2014. Despite the 12 January announcement of the r cabinet nominees, Ghani and Abdullah have yet to win legislative approval for all of those nominated or resolve the final details of their shared political powers derived from their national unity government agreement. Resolving these issues will require continued international engagement and support.

International financial aid remains the most important external determinant of the Kabul government's strength. However, the slow economic recovery from the global financial crisis has created fiscal challenges for many of Afghanistan's primary donors, particularly in Europe and Japan. These economic hurdles at home have reduced donors' enthusiasm and capacity to provide Afghanistan additional long-term financial aid above levels pledged through 2017 and reaffirmed in 2014 at the London Conference and NATO Wales Summit.

The Afghan National Security Forces (ANSF) prevented the Taliban from achieving a decisive military advantage in 2014. The ANSF, however, will require continued international security sector support and funding to stave off an increasingly aggressive Taliban insurgency through 2015. The ANSF, with the help of anti-Taliban powerbrokers and international funding, will probably maintain control of most major population centers. However, the forces will most likely cede control of some rural areas. Without international funding, the ANSF will probably not remain a cohesive or viable force.

The Taliban will probably remain largely cohesive under the leadership of Mullah Omar and sustain its countrywide campaign to take territory in outlying areas and steadily reassert influence over significant portions of the Pashtun countryside, positioning itself for greater territorial gains in 2015. Reliant on Afghanistan's opiate trade as a key domestic source of funding, the Taliban will be able to exploit increasing opium poppy cultivation and potential heroin production for ready revenue. The Taliban has publicly touted the end of the mission of the International Security and Assistance Force (ISAF) and coalition drawdown as a sign of its inevitable victory, reinforcing its commitment to returning to power.

Pakistan

Pakistan will probably continue to implement some economic reforms and target anti-Pakistan militants and their activities.

- Prime Minister Sharif's promises to address economic, energy, and security issues almost certainly fell short of high public expectations. Furthermore, his standing weakened when he reportedly asked the Army to step in and handle opposition protests in late 2014.

- We assess that Islamabad will approve some additional economic reforms in 2015. Undertaking future economic and energy reforms will be more challenging and will probably face greater political and popular opposition.

- The Pakistan Government will probably focus in 2015 on diminishing the capabilities of the Tehrik-i-Taliban (TTP), which claimed the attack on a school in December - leaving over 100 children dead.

We judge that Pakistan will aim to establish positive rapport with the new Afghan Government, but longstanding distrust and unresolved disputes between the countries will prevent substantial progress.

- Pakistan's provision of safe haven to Lashkar-e Tayyiba will probably continue to be a key irritant in relations with India.

India

Prime Minister Narendra Modi's decisive leadership style, combined with the 2014 election of an absolute majority in the lower house of Parliament of his Bharatiya Janata Party (BJP), will enable more decisive Indian decisionmaking on domestic and foreign policy. Although India has a long-standing position that it maintain an independent policy, Modi will probably seek to work more closely with the United States on security, terrorism, and economic issues.

India wants to maintain a stable peace with Pakistan but views Pakistan as a direct terrorism threat and a regional source of instability.

India is concerned about the stability of Afghanistan and its own presence there following the drawdown of international forces and is looking for options to blunt the influence of Pakistani-supported groups and ensure that Afghanistan does not revert to a haven for anti-Indian militants.

Indian leaders will almost certainly pursue stronger economic ties with China that support the government's economic agenda of closing the trade gap and attracting investment in infrastructure. New Delhi's concern over perceived Chinese aggressiveness along he disputed border and in the Indian Ocean is probably growing in light of border incidents and the visit of a Chinese submarine to Sri Lanka in 2014.

SUB-SAHARAN AFRICA

Sub-Saharan Africa will face political and security challenges in 2015 including numerous presidential elections, ongoing insurgencies, and continuing intrastate conflict. The ongoing Ebola virus epidemic will undoubtedly challenge both Western African nations and the larger international community in trying to contain the virus' spread and counter economic degradation in fragile West African nations. Stability in South Sudan, Nigeria, Somalia, and the Central African Republic (CAR) will almost certainly remain tenuous throughout 2015.

West Africa

The Ebola virus will persist throughout West Africa in 2015, posing a significant threat to the economic viability and consequently the stability of the region. The continued drain on resources and unprecedented need for medical personnel will strain governments and economies in Liberia, Sierra Leone, and Guinea—the three worst-affected countries. Sustained financial and materiel assistance from the international community, continued domestic support for the governments' anti-Ebola efforts, and community engagement to change local misperceptions about the disease's cause, treatment options, and burial practices will remain critical to slowing the epidemic. Economic growth in the outbreak zone has already slowed and will continue to slow during 2015, straining budgets and probably increasing dependence on international donor aid. A prolonged or severe outbreak that continues well into 2015 might prompt Guinea to delay Presidential elections, increasing the possibility of election-related violence. Military and security services in the key outbreak countries will probably successfully contain isolated unrest and local hostility toward Ebola-response personnel.

Sudan

Khartoum will almost certainly confront a range of challenges, including continued insurgencies in the periphery, public dissatisfaction over continued economic decline, and potential protests surrounding its April 2015 elections. Sudanese economic conditions since South Sudan's independence in 2011 continue to deteriorate. Such conditions, including rising prices on staple goods, fuel opposition to the Sudanese Government.

South Sudan

Clashes between opposition forces and the Sudan People's Liberation Army

(SPLA) will almost certainly increase during the dry season—which lasts from November to April—undermining ongoing peace talks and putting tenuous humanitarian gains at risk. Peace talks between Juba and opposition elements will probably remain slow-going.

Nigeria

Instability in Nigeria will probably increase in 2015, given contentious elections delayed until March and April, plummeting oil revenue, and the military's inability to check Boko Haram's ascendancy in the northeast. The election will occasion violence, with prospects for protests in the months following the election. In addition, militants might remobilize in the Niger Del a and attack the oil industry. Boko Haram will probably continue to solidify control over its self-declared Islamic state in northeastern Nigeria and expand its terror campaign in neighboring Nigerian states, Cameroon, Niger, and Chad. Abuja's reliance on oil exports for revenue will almost certainly ensure that Nigeria remains vulnerable to fluctuations in the global oil market in 2015. Declining oil prices will probably squeeze government revenues and drain currency reserves. Abuja's overtaxed security forces will have e limited ability to anticipate and preempt threats.

Somalia

In Somalia, al-Shabaab is conducting asymmetric attacks against government facilities and Western targets in and around Mogadishu. The credibility and effectiveness of the young Somali Government will be further threatened by persistent political infighting; ill-equipped government institutions; and pervasive technical, political, and administrative shortfalls.

Lord's Resistance Army

The Lord's Resistance Army (LRA), even in its weakened state, probably has the ability to regenerate if counter-LRA operations are reduced. The LRA continues to display great agility in its geographic areas of operation and in the operational security of its activities.

Central African Republic

Despite the presence of international peacekeeping forces, the risk of continued ethno-religious clashes between Christians and Muslims throughout the country, including in the capital, remains high.

The Sahel

Governments in Africa's Sahel region—particularly Chad, Niger, Mali, and Mauritania—will remain at risk of terrorist attacks and possible internal conflict. Al-Qa'ida in the Lands of the Islamic Maghreb (AQIM) and affiliated groups are committed to continuing their terrorist activity in the Sahel, including against Western interests. They will probably seek to increase the frequency and scale of attacks in northern Mali. Sahelien militaries will struggle to handle a wide array of security threats.

LATIN AMERICA AND THE CARIBBEAN

Cuba

Cuban President Raul Castro's focus will almost certainly be preparing the country for the eventual end of the Castro era and maintaining tight political control. He is cautiously implementing economic and leadership reforms and released dozens of political prisoners in early January. Cuba's principal interest in normalizing relations with the United States is probably linked to its recognition of the need to ease discontent over dismal living conditions and poor economic prospects. The slow rollout of economic reforms and a fall in nickel output cut GDP growth to 1.2 percent in 2014. Crucial components of the economic reform program—reducing the state role in the economy and opening up a few opportunities for self-employment—will probably produce numerous, short-term economic dislocations before gradually increasing productivity and jobs.

Cuba's population of 11 million has been declining since about 2005 because of falling birthrates and emigration. Cuban migrant arrivals at the US southwest border rose from 10,400 in FY12 to 17,300 in FY14. Maritime arrivals and interdictions will probably increase in 2015 because of rumors that if the two countries normalize relations, the United States would change immigration policies that allow Cubans who reach the United States to obtain status.

Central America

Weak institutions, poor economic prospects, and the growing strength of criminal gangs will probably limit the ability of the governments of Central America's northern tier —El Salvador, Guatemala, and Honduras—to improve rule of law, job opportunities, and citizen security, which will probably continue to fuel immigration to the United States in 2015. Fractured legislatures, political challenges, and entrenched business interests will probably slow agreement on raising soma of the lowest tax collection rates in the world or adopting economic and social policies that would help -educe the high rates of poverty that spur migration to the United States. About 25 percent of El Salvador's population has emigrated during the past two decades, mostly to the United States, because of lack of economic opportunities and widespread insecurity. El Salvador's economy has experienced the lowest economic growth rates in the region for eight consecutive years. Guatemala's weak fiscal position will undermine efforts to ameliorate extreme poverty, particularly in rural areas. About 1.6 million Guatemalans reside in the United States and send about $5.5 billion in remittances back home each year. Honduras, one of the hemisphere's poorest countries, is struggling to make headway against ineffective, corrupt institutions. Honduras has the world's highest rate of homicides per capita, despite a repotted modest decline in 2014, and criminal gangs are forcibly recruiting youth and extorting businesses and individuals.

Venezuela

Like most oil-exporting nations, Venezuela is experiencing the economic consequences of policy choices and the decline in global oil prices. Oil accounts for about 95 percent of Venezuelan export earnings and 45 percent of government revenue. Caracas will face a strained fiscal environment in 2015 along with rising inflation and shortages of essential goods.

Legislative elections are slated to occur by the end of 2015; voters will be concerned about public security, the economy, and political rights. President Nicolas Madura appointed a presidential commission to review the country's police system and recommend reforms after the high-profile murder of a national assembly deputy and a violent law enforcement confrontation in October 2014 with a radical, armed group known as a colectivo.

Haiti

Political tensions between Haitian President Martelly and his opponents will probably flare during 2015 and might undermine preparations for overdue local and parliamentary elections as well as for the vote for a new president in November 2015. Haiti will need substantial technical and financial support from the international community to organize and hold elections. Some violent protests are probable and might become more intense or widespread if political opponents believe that electoral preparations favor Martelly's party or allies.

* * * * * * * * * * * *

Editor's Note: The work of government agencies included in this compilation is not subject to copyright protection.

The contents of the documents reproduced here are solely the responsibility of the originating government agency. We make no claims, promises or guarantees about the accuracy, completeness, or adequacy of the contents, and disclaim liability for errors and omissions. No federal agency bears any responsibility for formatting or other errors contained therein, and proceeds from the sale do not go to the government. Of course, no warranty of any kind is given with respect to the contents.