Cyber Physical Systems
The Coming Singularity

By Marty Trevino

At this moment, a subtle but fundamental technological shift is occurring that is uniting our digital and physical worlds at the deepest architectural and operational levels. This technological shift will alter the global business, government, military and intelligence ecosystems. It is nothing less than a technological singularity and this technology will forever change our world—it is called Cyber Physical Systems (CPS).

This ill understood technological singularity is easily dismissed through cognitive error by strategic decisionmakers who are inundated by cries of technological revolution on a weekly basis. Yet, Silicon Valley visionaries, former National Security Agency (NSA) Senior and Technical Officers, and Tier 1 researchers are comparing this technological shift to a "black swan" event and when assessing its effects, are placing it in the "Unknown / Unknown" category of former Secretary of Defense Donald Rumsfeld's quadradic event characterization schema.[1]

Cyber Physical Systems are at the center of the unification of what have always been distinct physical and virtual worlds. And while the convergence of our physical and virtual worlds is not conceptually new, it is the capability which CPS possess that creates one of the greatest intellectual and technical challenges of our time. Cyber Physical Systems are creating "open systems" able to dynamically reconfigure, reorganize and operate in closed loops with often full computational and communication capability. Machine Learning can be fully integrated within a CPS network and this will soon be followed by partial, and eventually full, Artificial Intelligence—often without the ability of humans to observe the ongoing processes of the system. Cyber Physical Systems are at times even composed of unconventional computational and physical substrates such as Bio, Nano, and Chemical. It is the convergence and morphing of the physical and cyber worlds into multi-agent, intelligent CPS that constitutes nothing less than the technological singularity of our time.

Dr. Marty Trevino works for Fortinet in the office of the CISO as the Senior Director of Security Strategy. He previously served as the Technical Director of Mission Analytics for the National Security Agency of the United States.

Tech Hype and Buzzwords or the Unknown/Unknown

No industry enjoys creating hype more than the technology industry. Every new mobile App, computer program, algorithm, machine learning construct, etc. is dubbed as revolutionary and destined to change the world. The reality is that very little of this hype is accurate; but this does not violate the premise that "black swans" do exist and when they are discovered, they are highly impactful. CPS is today not only highly impactful and seemingly improbable; but in the framing of Rumsfeld, CPS also falls into the Unknown / Unknown category. Simply put, we ignore this technological shift at our peril and open the door to our adversaries who do not ignore this shift.

The fact that we are entering a CPS and Internet of Things (IoT) dominated world is beyond debate. That we do not have the level of understanding required regarding the effects of CPS on the world is also beyond debate. Nor do we have a clearly defined way of attaining the necessary level of understanding required to embark upon military and intelligence operations in foreign cyber space dominated by these systems. These realities present both strategic challenges and opportunities. Attaining the level of understanding of CPS to enable complex operations with designed effects is this generation's equivalent of breaking Enigma; and the strategic implications of doing so are equally great.

Defining and Characterizing Cyber Physical Systems (CPS)

In 2013, a consortium of European experts from France, Germany, Italy, Sweden, the UK, and other nations came together with the main objective of expanding European competence in embedded mobile and the network controls of the evolving class of unionized systems.[2] They called themselves CyPhERS and they set out to define, conceptualize and even model one of the greatest intellectual challenges of our time—the concatenation of the virtual and physical worlds into what has become known as Cyber Physical Systems (CPS).

Cyber Physical Systems represent the coupling of two distinct worlds and their subsets to include: industrial and operational technology, building automation, the Internet of Things (IoT), high speed connectivity (4G and soon to be 5G), cloud and machine learning (ML), all made supremely effective with feedback loops and within cutting edge new architectures. The term "cyber-physical systems" is generally credited to Helen Gill, Program Director for Computer and Network Systems at the National Science Foundation. Gill coined the term somewhere around the year 2006 to characterize the intersection of the physical and cyber worlds. Cengarle et al., notes that CPS is subject to numerous interpretations depending upon the individual lens through which the technology is viewed. The deep penetration of electronics, sensors, and software into every aspect of modern life is referred to in unique nomenclature by the varying communities which are served by those advances. Some of these include: IoT, the 4th Industrial Revolution, Smart Cities, Home Automation, Digital Medicine, etc. The CyPhERS group realized that an expanded view, and thus definitions, of those systems were necessary based on the perceived disruptive potential of multi-agent, intelligent Cyber Physical Systems.[3]

The National Science Foundation provides a base definition for CPS that is widely accepted today:

> *A Cyber Physical System is a mechanism that is controlled or monitored by computer-based algorithms, and tightly integrated with the Internet and its users. CPS systems tightly intertwine the physical and software components, each operating on different spatial and temporal scales, while exhibiting multiple and distinct behavioral modalities.*

This dynamic and complex interaction is agile, and changes based on the context."[4]

Cyber Physical Systems will encompass the entire spectrum of technical systems from tiny to massive in scope and size. Torngren et. al., more over characterize CPS as "inherently multidisciplinary and multitechnological, and relevant across vastly different domains, with multiple socio-technical implications."[5] The strategic implications of this technological shift must be made clear for U.S. military and intelligence operations, in particular at the nation state level where understood mastery of this tradecraft is in itself a deterrent to adversaries.

A Dependent Relationship

The conceptual integration of the physical and cyber domains is not new. It is the scale, multi-agent nature, system intelligence level of integration, and the cross cutting of domains which characterizes Cyber Physical Devices that is both novel and relevant. In conceptualizing what constitutes CPS, and thus what will eventually engender itself in every physical and virtual ecosystem, it is important to note that CPS is the result of a dependent relationship between the Core, Endpoint, Connectivity, and Cloud. CPS are not any single piece of technology; rather the complex integration of devices and architectures made possible by the explosion in Endpoint devices, increases in Connectivity speeds, and the expansion of Cloud capabilities to, at times, include High Performance Computing and embedded / native Machine Learning. CPS is thus networking at multiple and extreme scales, and multiple temporal and spatial scales—at times simultaneously.

Initially triggered by the marriage of Industrial and Operational Technology, CPS now consumes Building Automation (BA) and is enmeshed with the Internet of Things (IoT). Critical to understanding the opportunities and threats of CPS is that when these technologies are combined, they constitute something infinitely more capable than the individual parts.

Cyber Physical Systems (CPS) and the Internet of Things (IoT)

When discussing Cyber Physical Systems, often the first question to arise is how CPS differs from the much talked about Internet of Things or IoT? Is CPS simply hype or an alternative nomenclature for the IoT? The answer is "no." The differences between CPS and the IoT are significant and important to understand.

The Internet of Things (IoT) refers to the massively expanding number of physical devices that feature an IP address enabling internet connectivity and thus, communication between devices and larger systems. These devices range from home speakers to appliances to thermostats. Sedlar et al. state that the "Devices classified as IoT devices are typically connectivity-centric, advocating the best-effort nature of the internet itself, while computation is secondary and, in many cases, minimal."[6] Cyber Physical Systems differ greatly in that they "use shared knowledge and information obtained from sensors to independently control physical devices and processes in a closed loop."[7]

Cyber Physical Systems are defined by highly integrated computation networks, closed loops, and physical processes. CPS can have multiple temporal and spatial scales, as well as be networked at extreme scales. Cyber Physical Systems are multi-agent and often intelligent, with the ability to dynamically reconfigure and reorganize. The result of these combined characteristics is high degrees of automation, and capabilities far exceeding simple communication and the simple nature of IoT devices. CPS is also now perceived as being a primary vector for the IoT to connect with higher order functions. It is this dynamic integration and connection of disparate devices and systems that present tremendous opportunity for both U.S. advocates and adversaries.

Next Generation Analytics—Understanding and Common Operating Pictures

It is written in the Old Testament that King Solomon went to God and asked to be the wisest of all kings. God granted his wish by giving him "understanding." The advancement of CPS and the capabilities they bring presents massive technical and non-technical challenges from the lens of understanding. Among the most easily constructed approaches to developing an understanding or "internal model" from a neuroscience perspective is a deconstructivism-based approach. A deconstructivism approach can be taken in framing this challenge to begin with defensive challenges and offensive opportunities. This framing can then be extended into military networks, kinetic and non-kinetic operations, denial of intent, and the deriving of other effects in the eco-system. Yet, this sort of endeavor, while useful, fails to incorporate a decisionmaker's best asset—Advanced Visual Analytics.

The importance of Visual Analytics to inform common operating pictures and internal models of strategic decisionmakers is widely recognized in the U.S. military and Intelligence Community. Few decisionmakers are not interested in "seeing the data." But seeing the data at meaningful levels of analysis around the IoT and CPS is no simple endeavor. The sheer size of the IoT and complexity of CPS fuels the problems associated with analytics at scale. The problem of analytics at massive scale encompasses both technological challenges and higher order human functions.

Visualizing millions of CPS and IoT devices in a way that informs and facilitates strategic decision-making is a massive challenge for technical experts. At the highest level of analysis this challenge is not new; Uber, Facebook, Twitter, and Google track the movement, activity, and use of millions of devices in near real-time. The challenge becomes fully exposed when altering the use cases to those of a military and intelligence nature. In each of these cases / domains, how to visualize massive amounts of data in a way that underpins human decision cycles with time as a principle variable in the equations remains unsolved. The element of time as a variable cannot be understated, as with each passing minute the number of devices and actions performed increases in a power curve distribution fashion. The reality of scale and time in relation to temporal opportunities and strategic understanding of a dynamic ecosystem opens the door to mandatory discussions of Machine Learning and fully automated decision-making. And yet, the notion of eliminating humans from the decision loops is strongly rejected by those with decision authority today in virtually every domain. Decision cycles or OODA loops (observe–orient–decide–act), as they are commonly referred to, remain a human-centric process informed by data, analytics, and visualizations. Unfortunately, to believe that human beings will be able to make sense of trillions of actions over periods of time and make accurate, timely decisions can be likened to attempting to build a new Maginot Line in an age of precision weapons; advanced analytics and Machine Learning are the keys to building capability to "sense make" in a world dominated by the IoT and Cyber Physical Systems.

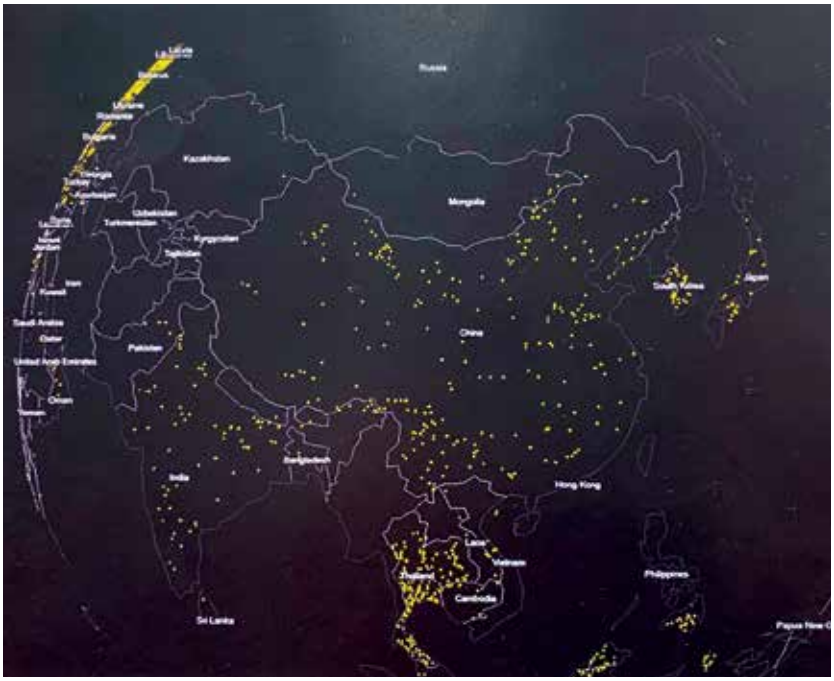
To understand the necessity of developing the next generation object visualization and incorporating Machine Learning (ML and eventually Artificial Intelligence) into the decision process, it is useful to examine a set of current state-of-the-art network visualizations. Consider the visualizations in figures 1-3 to represent both CPS networks and clusters of IoT devices related to those CPS networks across a nation state. Each dot on the map represents a network of no less than 100 CPS for a single industry. In this case, we will consider Oil and Gas facilities at a single point in time to be the target set. The relatively few "dots" reinforces the belief that as an individual or team of people, the target set can be

understood. At this level of analysis, the ability to dynamically "drill down" into the clusters is possible by human analysts and a dedicated team of "experts" could likely glean goodness out of the data.

In this second view (Fig. 2), another single target set of critical infrastructure is visualized. And while the number of networks has increased, as has the dispersion across the nation state (both present challenges from a targeting perspective), size and scale are not insurmountable. Meaningful analysis can still be done in both automated and manual methods and strategic decision informed. The issue is that neither of these views (CPS networks) exists in isolation and the associated IoT devices are not yet shown. To target these networks, one must show contextual networks of CPS systems and affiliated IoT devices.

The final illustration (Fig. 3) is an accurate and complete visualization of both CPS networks and IoT clusters of 10,000 devices or more.

Figure 1. CPS Networks and IoT Clusters—View 1.



Source: Illustration generated by author

Figure 2. CPS Networks and IoT Clusters—View 2.

Source: Illustration generated by author

Figure 3. CPS Networks and IoT Clusters—View 3.

Source: Illustration generated by author

When assessing this level of information density, the human brain is likely to default to a "prone to error" System 1, and these errors have cost U.S. intelligence officers and military commanders dearly across the many wars fought by American warriors. Yet, it is precisely this density of objects that must be dealt with in all future scenarios. In this visualization rendering, only simple presence was considered, device behavior (features) was omitted and time was held to one minute. If we are to capture 100 features from these networks multiplied by the number of devices and networks over a 24-hour period, the complexity challenge becomes clear. Simple decomposition approaches and manual analysis undertaken by even legions of smart people will no longer suffice.

We stand at the event horizon of a technological singularity that, if we are to be "left of boom," an entirely new generation of visual analytics and applications of Machine Learning will be required to inform and perform strategic decisionmaking at speed and scale.

Next Generation Analytics and High Dimensional Space

Military commanders and senior intelligence officers have been quick to realize that advanced analytics are among the keys to situational awareness and successful operations. This truism will only become increasingly obvious as CPS and the IoT mature. Next generation analytics will provide strategic advantages at all levels, but will

fundamentally underpin creative decision processes and higher order human decision functions, such as the weighing of risk and sequencing of kinetic operations. Among the promising and novel approaches to next generation visual analytics is the use of Object Based Analysis (OBA), High Dimensional Space (HDS), and High-Performance Computing (HPC). In considering devices and even networks as objects, features association becomes a powerful tool enabling rich contextual information to be associated with a core object. Adopting this approach enables the creation of unique visualizations designed to capture the inherently dynamic nature of the network and allow the user to interact with the data in ways fundamentally different than what is possible with two dimensional graphs / charts.

Machine Learning, in its various forms, can be unleashed on these data sets with correlations, relationships, and actionable opportunities discovered at speed and scale. These insights can also inform decisionmaking at all levels, but with an emphasis on strategic decisionmaking, as this is fundamentally a creative process in the human brain. It is believed that the outcome can be a new level of understanding for senior commanders, as well as fully automated decision authority for the coming generation of Artificial Intelligence.

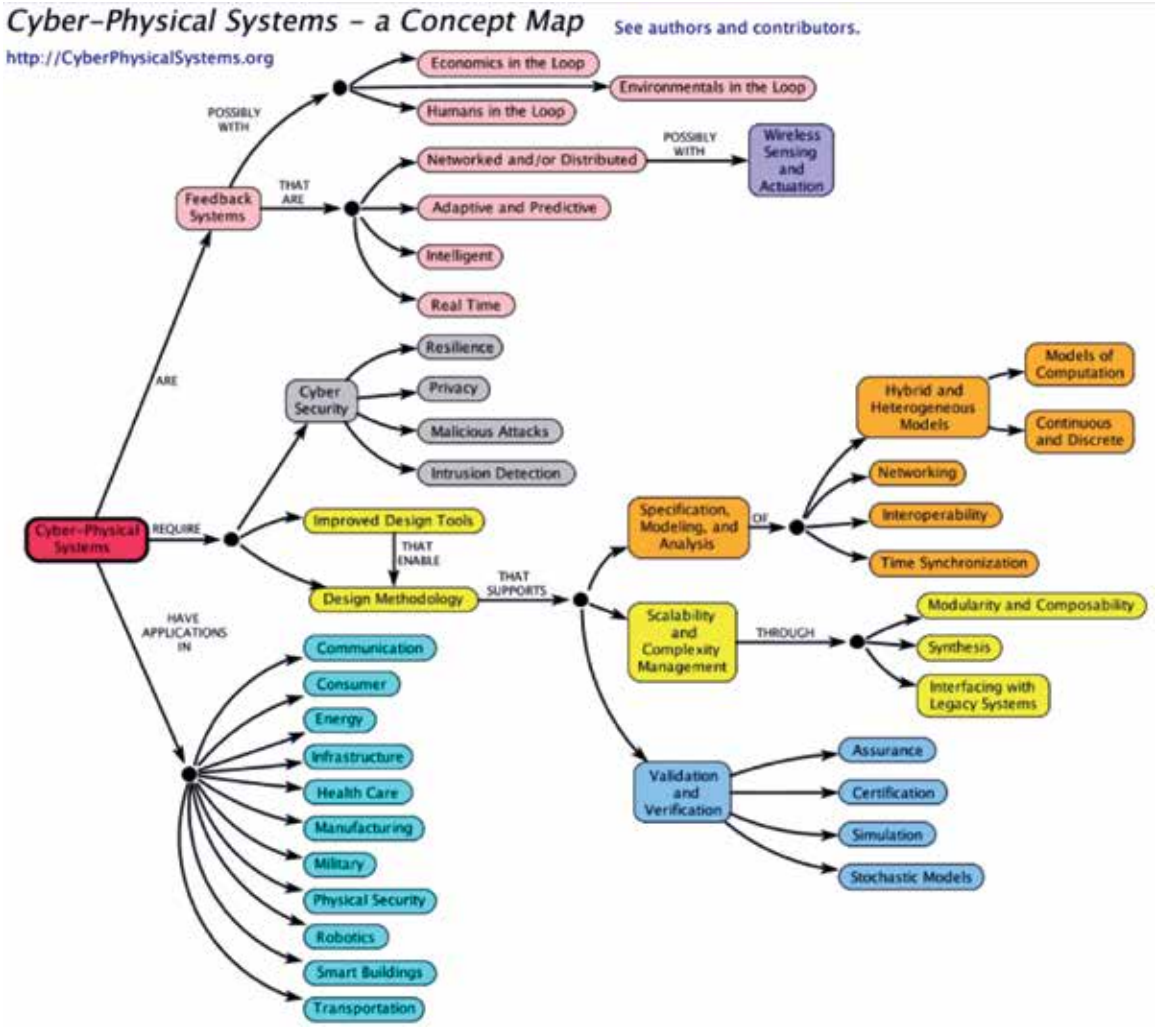
In the most advanced analytic environments, it is possible to stand in the cluster and interact with the visualization in three dimensions by touch and natural language voice processing. The precise benefits of this are currently unknown; but from the lens of the neuroscience of decisionmaking, the possibility to impact the Cortex, Visual Cortex, the Thalamus and hence the formulation of the Internal Model itself is promising. It is possible that even the Amygdala, which plays a decisive role in memory creation, and its ability to override other areas of brain function in moments of extreme danger may be influenced by interacting with data over time in HDS. A theorized outcome would be the creation of "richer" memories also serving to influence the Internal Model for dealing with future high-risk events. Thus, both the technical aspects of analytics at scale and the human brain's ability to process data and make decisions are components in the next generation of visual analytics. To the winner of this race goes the high ground of understanding in rapidly evolving nation state level actions in cyber and any kinetic conflict.

Conceptualizing a CPS / IoT Ecosystem

Attempting to conceptualize a tightly integrated physical and cyber world while it is rapidly evolving can be likened to building an airplane in flight. And while this is not a new conundrum, it has been made markedly more difficult due to scale, speed of development and deployment, as well as the attributes of CPS. Accurately conceptualizing or "framing" the evolving Cyber Physical, or CyPhy, world we must operate within is perhaps the most difficult technical and intellectual endeavor of our time.[8] This intellectually "deep" undertaking is easily dismissed by those in leadership positions as a task to be left to others as "more pressing things" must be attended to. And while there is some truth to this perception, it also can engender the unintended outcome of allowing old Internal Models of the ecosystem to remain intact in the face of a rapidly developing environment; thus, promoting decisions not based on the latest understanding. This tendency to avoid the intellectually deep and difficult foundational work is compounded by the uniqueness of the military and intelligence communities' Use Cases.

The default of many leaders has been to simply adopt frameworks composed by commercial industry or academics. And while this approach can certainly begin the process of framing, from a military and intelligence perspective, it can only be the initial step of developing the required level of understanding.

Figure 4. Cyber–Physical Systems, a Concept Map.



Source: The Ptolemy Project, UC-Berkley, available at <https://ptolemy.berkeley.edu/projects/cps/>.

More robust frameworks have risen out of academic institutions and think tanks. Some of these frameworks have attempted to specifically isolate the component and function relationships of CyPhy. These maps are considerably more useful in illustrating simplistic relationships and the potential interaction of devices and closed loop systems. Yet, even the most robust of these is woefully simplistic in the face of the complex Use Cases of the U.S. military and intelligence services.

At its core, virtually all military and intelligence planning is action oriented. Thus, seeking out existing frameworks which can underpin action can expedite the framing process. In 2010, the McKinsey Institute created a simple, but effective framing of IoT devices which also has application to CPS. This unique stratification is another high level, but useful step in creating a complex framework to underpin operations.

Considerably more work is needed to create the required level of understanding of the singularity we

Figure 5. IoT Device Application Framework .

Information and analysis			Automation and control		
1 Tracking behavior	**2 Enhanced situational awareness**	**3 Sensor-driven decision analytics**	**1 Process optimization**	**2 Optimized resource consumption**	**3 Complex autonomous systems**
Monitoring the behavior of persons, things, or data through space and time	Achieving real-time awareness of physical environment	Assisting human decision making through deep analysis and data visualization	Automated control of closed (self-contained) systems	Control of consumption to optimize resource use across network	Automated control in open environments with great uncertainty
Examples: Presence-based advertising and payments based on locations of consumers	Example: Sniper detection using direction of sound to locate shooters	Examples: Oil field site planning with 3D visualization and simulation	Examples: Maximization of lime kiln throughtout via wireless sensors	Examples: Smart meters and energy grids that match loads and generation capacity in order to lower costs	Examples: Colision avoidance systems to sense objects and automatically apply brake
Inventory and supply chain monitoring and management		Continuous monitoring of chronic diseases to help doctors determine best treatments	Continuous, precise adjustments in manufacturing lines	Data-center management to optimize energy, storage, and processor utilization	Clean up of hazardous materials through the use of swarms of robots

Source: *McKinsey & Company, "The Interntet of Things," McKinsey Quarterly (March 2010), available at* <https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things>.

now face. It is no doubt that more robust frameworks exist at the classified levels and should be sought out through the appropriate channels. It is useful to revisit the wisdom of Albert Einstein who is quoted to have said—"If I had an hour to solve a problem, I'd spend 55 minutes thinking about the problem and five minutes thinking about solutions."

Technological Advances and Implications for U.S. Forces

The operationalization of Cyber Physical Systems on a global scale presents a duality which has few intellectual and conceptualization parallels in today's technical world. CPS also represents one of the greatest opportunities for the U.S. military and intelligence services to create ecosystem effects through non-kinetic operations. These effects can range from influencing foreign decisionmaking to denying an adversary the ability to operate and/or sustain operations against U.S. forces world-wide.

In conceptualizing the possibilities for affecting adversary ecosystems, a principle consideration is that the United States and Europe are leading in the deployment of CPS. Thus, it is possible to evaluate these deployments from a "strengths, weaknesses, opportunities and threats (SWOT)" perspective, and mirror anticipated deployments by our adversaries (understanding of course the differences in Russian or Chinese power grids as an example).

This type of analysis is not new and can simply be applied to CPS development into the kinetic realm. An example of anticipated CPS development

in the kinetic realm can be found in the coupling of high-speed encrypted connections linking multiple platforms. The F–35 Joint Strike Fighter is designed to receive direct data feeds from on station Global Hawks, interpret this data and transmit targeting and prioritization of targets to missile-carrying F–15, F–16 and F–18s. The result of this tight integration through CPS is to enable precise adversarial prioritization and targeting at speed and scale in high-end conflicts. Foreign nations, such as India, have fully integrated high-speed data links in their fighter force. Indian Sukhoi (SU)–30 MK 2s are frequently observed communicating through these modes. This falls short of a full CPS system, but clearly highlights the development path (which mirrors the U.S. path) which will be taken. This understanding should not be squandered, and analysis performed through both SWOT capability and progression lenses.

In the future, CPS will enable the full automation of robotic systems with wide ranging kinetic capability. One often discussed example is swarm bots with full ranging mission parameters. These include bots designed to confuse adversary targeting systems, while dedicated attack units eliminate enemy units. All of this will be done at cyber speed and on a global scale, with humans in and out of the loop. Both the military and the intelligence community will benefit from the applications and/or compositions of new physical substrates such as Smartdust. Smartdust represents novel applications of micro-electromechanical and even biological systems such as sensors, as well as intelligent bots to detect a wide array of inputs and outputs. Smartdust can be distributed over an area to detect prescribed environmental elements—temperature, light, vibration, etc. usually through radio-frequency identification. Initial tests have been highly successful, thus opening the way to further innovation in this field potentially providing novel vectors to pinpoint situational awareness to U.S. forces or intelligence operations.

CPS are rapidly penetrating and will eventually permeate all military and critical infrastructure verticals of every country. Understanding the deep penetration of CPS into these domains is critical to the success of U.S. forces. It is always preferable to deny the adversary the ability to operate or effectively engage in kinetic operations versus engaging in combat operations with a well-prepared and capable enemy.

Simply put, U.S. forces face an endless set of scenarios in which an infinite number of small and separate systems can work in cooperation to achieve much larger military and intelligence objectives.[9]

CPS Analytics and the Art of the Possible

Advanced analytics provide strategic advantages that are difficult to counter in both the military and intelligence domains. It is an understatement to say that there is significant interest in what next generation analytics will look like and do for decisionmakers. Yet, there is a massive misconception as to the future of cyber (CPS and IoT) analytics which stems from purist thinking in the technical realms and misconceptions in the minds of senior decisionmakers. The question, "what will drive next generation analytics?" is likely to generate several permutations of the same set of bullet points. The list of concerns ranges from the "quality of the data," "trust in the data," "data precision," "speed of analysis," "eliminating bias in the algorithms," "story-telling of the data," "good dashboard design," "data" density ratios," etc. And while all of these are important, they all pale in importance to the neuroscience of decisionmaking. There are two scientific dimensions of decisionmaking which are not considered today but will be addressed two generations from today; these are the Umwelt and the Internal Model.

The Umwelt is the spectrum of information which a living being can sense and process.[10] The Umwelt represents the biological foundations at the

epicenter of both communication and understanding in all animals.[11] For a Tick, the Umwelt consists of the ability to detect heat and body odor, for the Eco Locating Bat, its world is largely constructed out of its ability to sense air compression waves. Humans have a variety of senses; but we are still severely limited in what we can sense – despite the belief that we see everything. Yet, our highly capable human brain can learn to utilize new senses and will in fact form new neural paths if necessary, to interpret these signals. These new information streams are then incorporated into our decision cycles and the formulation of our Internal Model of what constitutes the ecosystem we exist / operate within. It is here that the neuroscience of decisionmaking holds the key to next generation analytics and improved strategic decisionmaking versus improving data precision or designing better dashboards. Next generation analytics will not be better data or colors on a dashboard; but rather it will be augmented sensory sensation and individually centric Artificial Intelligence. Today, work is underway to develop wearable devices which can translate data into modulated pulses to be felt by the individual wearing the device. Next generation analytics will be "felt" as well as seen and the human brain will unconsciously know when "something is wrong" or "right." Augmented sensory sensation, coupled with Artificial Intelligence (AI), is the next generation high ground of analytics for U.S. military commanders and intelligence officers as they engage in a never-ending battle of wits with our adversaries.PRISM

Notes

[1] Taleb Nassim, *The Black Swan: Second Edition: The Impact of the Highly Improbable 2nd ed.* (New York: Random House Publishing Group, 2010).

[2] CyPhERS, "D6.1 +2—Integrated CPS Research Agenda and Recommendations for Action," 2015, available at <http://ww.cyphers.eu/>.

[3] M. Törngren, "Characterization, Analysis, and Recommendations for Exploiting the Opportunities of Cyber-Physical Systems," *Cyber Physical Systems: Foundations, Principles and Applications*, ed. Houbing Song et al. (San Diego, California: Elsevier Academic Publishing, 2016).

[4] National Science Foundation, "Cyber-Physical Systems Program Soliciation NSF-1015," 2010, available at <https://www.nsf.gov/pubs/2010/nsf10515/nsfl10515.htm>.

[5] Törngren, 4.

[6] Urban Sedlar et al., "Big Data Analysis and Cyber-Physical Systems,"*Cyber-Physical Systems, a Computational Perspective*, ed. Gaddadevara Matt Siddesh et al. (New York: Taylor and Francis Group, 2016).

[7] Aaron D. Ames, Paulo Tabuado, and Shankar Sastry, "On the Stability of Zeno Equilibria," Lecture Notes in Computer Science Series, Vol. 3927, "International Workshop on Hybrid Systems Computation and Control, 2006," as referenced in "The Internet of Things," McKinsey Quarterly, October 2010, available at <https://www.mckinsey.com/industries/high-teck/our-insights/the-internet-of-things>.

[8] The term "CyPhy" is credited to Phil Quade, former NSA Cyber Task Force Director and current Fortinet® Chief Information Security Officer.

[9] Daniel Khaneman, *Thinking Fast and Thinking Slow, 1st ed.* (New York, NY. Farrar, Straus and Giroux, 2011).

[10] Umwelt loosely translates to English as the "Surrounding World".

[11] Thomas A. Sebeok, "Contributions to the Doctrine of Signs," *Studies in Semiotics Series*, Vol. 5 (Bloomington, Indiana: Indiana University Press and The Peter de Ridder Press, 1976).