Towards a Cyber Common Operating Picture

Gregory Conti
Cyber Research Center
United States Military Academy
West Point, New York, USA

John Nelson
Cyber Research Center
United States Military Academy
West Point, New York USA

David Raymond
Cyber Research Center
United States Military Academy
West Point, New York, USA

Abstract: Commanders enjoy a refined common operating picture of the kinetic battlespace. While still imperfect, today's military command posts represent centuries of refinement and maturation enhanced by cutting-edge technology. Cyberspace's emergence as an operational domain, however, presents unresolved challenges to this status quo. Techniques for maintaining situational awareness and command and control of cyber operations, particularly joint cyber/kinetic operations, are ill-defined, and no current solutions provide military decision-makers with a comprehensive cyber common operating picture, or CCOP. This paper provides a framework for designing such systems. We focus on the problem of cyber-only operations as well as joint cyber-kinetic operations. Our analysis indicates that the CCOP problem is tractable, but non-trivial, requiring substantial effort realized through evolutionary and revolutionary research approaches.

Keywords: cyber operations, cyber COP, cyber Common Operating Picture, CCOP, cyber situational awareness

1. INTRODUCTION

Cyberspace's emergence as an operational domain challenges military organizations' current ability to provide commanders with enough critical information to lead operations involving cyberspace. This challenge rises from the inherent differences between kinetic warfare and combat realities in cyberspace. The days of a battlefield commander sitting in an operations center receiving staff briefings, which took hours to prepare, to make a handful of decisions that will take hours or days to execute, are anachronistic in the cyber warfare era. Unlike nuclear missiles, which take about 30 minutes for global transit, leaving time for hurried human decision-making, network packets take milliseconds. Thus, distance and reaction time approach zero in the cyber domain. Therefore, a cyber Common Operating Picture (CCOP) system that provides situational awareness despite cyberspace's largely opaque nature, enhances a leader's ability to make quicker critical decisions, and leverages automated responses that can operate at machine speeds is essential. Absent a CCOP, leaders are effectively blind to an entire operational domain where adversaries coordinate, operate, and hide. Significant advantage has historically gone to militaries that more effectively apply new technologies. Cyberspace is no different.

A CCOP's design is complex and must allow monitoring of the physical and virtual battlespace and provide actionable information. To prevent operator overload, such systems provide tailored and timely information at each military echelon. However, operators are not just passive observers of the battlespace, but are active participants, and the system must facilitate automated and manual Command and Control (C2) of kinetic and cyber forces. This paper provides a framework for the design of CCOP systems. Thus, we provide necessary underlying contextual information unique to the military domain as well as critical analysis of potential approaches. We do not claim an ultimate solution to this significant problem; we do, nevertheless, contribute a novel analysis of the problem space and a framework to inform future work.

We define *cyber* as the combination of Computer Network Attack (CNA), Computer Network Exploitation (CNE), Computer Network Defense (CND), and Global Information Grid Operations. Note that we explicitly omit the cognitive domain, i.e. information operations, but acknowledge that future CCOP systems will likely pursue this extension to parallel emerging military doctrine. We define *common operating picture* and *situational awareness* using U.S. military doctrine. A *COP* is "a single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness." *Situational awareness* is the "the requisite current and predictive knowledge of the environment upon which operations depend — including physical, virtual, and human domains — as well as all factors, activities, and events of friendly and adversary forces across the spectrum of conflict." Finally, *Battlespace* is an extension of the notion of the ground battlefield, to include air, land, sea, space, and importantly, cyberspace [1].

This paper is organized as follows. Section 2 places our research into the field of related work. Section 3 discusses the challenge of linking cyberspace and kinetic warfighting operations. Section 4 examines techniques for complementing visualization with machine processing. Section 5 analyzes key facets of a CCOP system's design. Section 6 provides our conclusions and suggests directions for future work.

2. Related Work

Important related work surrounds the creation of a CCOP, including work in network monitoring, intrusion detection, incident response, security visualization, and military command center design. This section highlights the work most germane to this paper.

Command centers began transitioning from physical map and acetate overlay to computerized displays in the 1990s. Military doctrine and technology have since significantly improved. For example, the U.S. military updated its doctrine to include significant coverage of

visualization and COP concepts, but only in the physical, not cyber, battlespace [2]. In terms of technology, the U.S. Army's blue force tracker system Force XXI Battle Command Brigade and Below (FBCB2) is representative of current systems that use GPS data to place military units on map-based displays. FBCB2 will upgrade into the Joint Battle Command - Platform (JBC-P), which provides mobile C2 and improved network communication capability. Tactical and operational command posts use Command Post of the Future (CPOF) to provide the battlespace COP from battalion- to division-level. CPOF provides a suite of tools for collaborative, real-time, multi-echelon C2. At the strategic and operational levels of war fighting, systems such as the Global Command and Control System (GCCS) provide a common operational picture including friendly and enemy status information. Other systems, such as the Advanced Field Artillery Tactical Data System (AFATDS) provide automated support for planning and controlling kinetic weapons, and other systems such as the Battle Command Sustainment Support System (BCS3) support logistics functions. Many deployable, hardened systems can survive austere environments, but require the space and consistent power of a command post or military vehicle; some systems, however, are battery-operated, handheld devices for battlefield usage, such as the Forward Entry Device (FED), linking artillery observers with fire support. Current systems represent the state-of-the-art in kinetic warfighting for situational awareness and for commanding weapon systems and subordinate units, but importantly, do not extend to the cyber domain.

Computer network monitoring does indeed occur in government and industry network operating centers, primarily designed to monitor network operation, and to a degree, to detect and defend against cyber-attacks [3]. They possess limited physical domain awareness, are primarily defensive, and lack offensive capabilities.

The speed with which decisions and actions must occur in cyberspace operations will increasingly surpass human capacity and already requires automated approaches. Consider the Defense Advanced Research Projects Agency's newly announced Plan X program. While limited details

are available, the program seeks "revolutionary technologies for understanding, planning, and managing cyberwarfare in real-time, large-scale, and dynamic network environments." Plan X emphasizes "visualizing and interacting with large-scale cyber battlespaces" and envisions "hardened 'battle units' that can perform cyberwarfare functions such as battle damage monitoring, communications relay, weapon deployment and adaptive defense." [4] Still in its genesis, research generated by this program will be germane to CCOP development.

Existing visual analytics tools may be integrated into a future CCOP system. Representative examples include IBM's Analyst's Notebook, which translates disparate information into actionable intelligence; Palantir, which fuses data from diverse data sources into a unified model to accelerate analysis and harden defenses; HP's ArcSight, which provides visibility into enterprise-level IT infrastructure; and Splunk, which allows multiple data source analysis, including logs, configuration files, and alerts; as well as the products of the start-up PixlCloud, which employ cloud resources to visualize and understand big data [5,6,7,8,9].

Academics are also developing visualization techniques suitable for potential CCOP integration. A full description is beyond this paper's scope, but we recommend studying the proceedings of the Symposium on Visualization for Cyber Security, the IEEE Visual Analytics Science and Technology Conference, the ACM Conference on Computer Supported Collaborative Work, and IEEE Information Visualization, for historical and emerging ideas. In addition, Conti's *Security Data Visualization* and Marty's *Applied Security Visualization* provide useful overviews of design techniques and insight into candidate visualization technologies [10,11]. Many of the visualization and interaction techniques useful for a CCOP exist today, but must be carefully integrated into a seamless system designed around large scale, potentially highly-automated, cyber warfighting needs.

Visualization is only part of a CCOP system, which also requires automated decision-making and analysis techniques. Butler suggests using decision analysis for cyber operations, which could be integrated into hybrid human-machine or machine-only cyber operations decision-making [12]. Butler's solution, or similar higher-level analytics, would likely become critical components in a CCOP system. In addition, as the future portends friendly algorithms fighting against enemy algorithms in the cyber battlespace, we suggest exploring Wall Street's high-frequency trading for important insights [13,14]. Finally, Boyd's classic work on decision-making and OODA loops might illuminate the dynamics of cyber warfare operations, particularly regarding human and machine cognition [15]. The CCOP must enable the user and the machine to cycle through the OODA loop faster than adversaries.

Our work's novelty springs from the gap between the robust military technology—excellent at tracking and issuing commands in the physical realm, but lacking cyberspace integration—and telecommunication industry systems, which monitor networks, but are unable to plan cyber operations, particularly if large scale and offensive in nature. A CCOP solution demands convergence and integration, but not all the required pieces exist today. Filling these gaps is the role of the CCOP systems we propose.

3. Linking Cyberspace and Kinetic Operations

The physical world and cyberspace differ dramatically. Geographic regions define the physical world, where military operations are divided into sectors of responsibility. Cyberspace is a manmade network whose components reside in physical space, but which is a complex and constantly evolving dynamic system modifiable by computer code. Minutes, hours, days define physical world's time. Cyberspace components can operate in milliseconds or less. For example, network packets travel near light speed, and computer code is executed by commodity processors at billions of operations per-second. The military marks physical world distance by meters and kilometers. Cyberspace

distance effectively approaches zero; the time-space differential is nearly negligible. Humans are slow, easily tire, and error-prone, but possess ingenuity. Computers can manipulate symbols for years and rarely make errors, but only on algorithmic problems. For additional discussion on these topics consult Miller's work [16].

In the land domain alone, military operations are incredibly complex, requiring a thorough understanding of enemy and friendly disposition, the current mission, and an executable vision. Maneuver, artillery, reconnaissance, and air defense activities must be deliberately synchronized with intelligence, engineer, communication, military police, and other supporting units. Modern U.S. military doctrine includes early steps toward integration of "soft" force, including information, psychological, and civil military operations, to influence the adversary and civilian populace. As the operation unfolds, forces seek to answer leaders' information requirements, take risk reduction and force protection measures, follow rules of engagement, and minimize negative environmental impacts. As casualties occur, supplies deplete, and systems break, force sustainment activities help maintain maximum operational potential. Simultaneously, signaleers seek to maintain reliable and robust communications [17]. Even the best plans, however, rarely survive initial enemy contact; all leaders—both friendly and adversary—must adapt. The result is Clausewitz's "fog of war," where combatants must make decisions with limited information while solving ill-defined problems, with limited time, and lives at stake [18]. Air, sea, space, and cyberspace operations are similarly complex and uncertain. To illustrate this complex environment, we offer the model in Figure 1, which demonstrates how cyberspace crosscuts the physical domains of air, land, sea, and space. While not an operational domain (in U.S. Military doctrine), we propose a second crosscutting plane for the electromagnetic spectrum, which acts as a substrate for some aspects of cyberspace. The CCOP's overarching objective is to link these domains in time and space into a single operating picture.

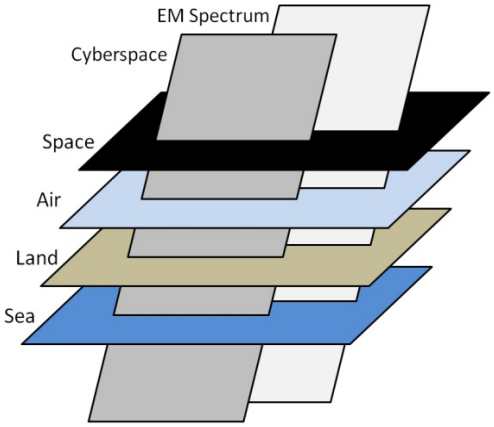

Figure 1. Cyberspace is unique among operational domains because it is manmade and crosscuts each physical domain, akin to a parallel dimension.

4. COMPLEMENTING COP VISUALIZATION WITH MACHINE PROCESSING

Visualization helps clear the proverbial fog of war. Carefully designed visualizations create windows onto information supportive of decision-makers by tapping into humans' high-bandwidth visual-recognition capacity. Visualization systems are far more than the graphical pie-and-bar charts found in office application suites. They are inherently interactive, contain carefully-crafted displays, and help users efficiently accomplish complex tasks. However, they are not the complete solution. Visualization systems tightly integrate humans into the loop, but while such systems enhance human decision-making, they still are significantly constrained by mankind's weaknesses. Over time, we anticipate the reduced utility of visualization systems alone because human intelligence and perceptual capabilities are constant, computer displays grow at a linear rate, but data requiring analysis has exploded exponentially. A scalable solution is to assign complementary CCOP tasks to human operators and machines, treating each as an integrated system. The right balance is critical. Human processing is in short supply and by nature limited in performance, so humans must perform their specialties (primarily pattern detection, analysis, and creative interpretation) and machines must operate as designed (speedily, accurately, and tirelessly

operating on symbols). The best solutions will come from humans' developing insights using visualization and then employing tools to structure this insight in ways that allow computers to do the bulk of future work. The reverse is also possible: machines can alert humans to information that requires human interpretation, see Figure 2. Think, for example, of malware analysts creating antivirus signatures. The signatures can then be automatically distributed across the entire enterprise antivirus system.

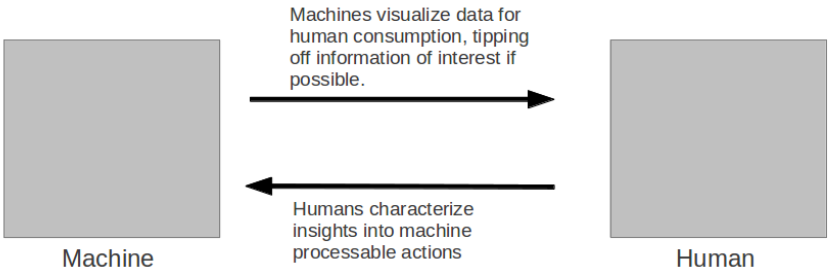

Figure 2. In a CCOP, humans and machines are complementary, tapping into mankind's high bandwidth visual processing system and applying the machine's tireless ability to follow algorithmic instructions.

5. GUIDING THE DESIGN

An effective CCOP system's design requires a deep understanding of system users and their operational environments. An understanding of user tasks, available data, and the available technology's capabilities is also crucial.

A. CCOP Users

Military organizations typically operate in three echelons: tactical-level (corps and below), operational-level (theater), and strategic-level (national), each with varying missions, capabilities, and areas of responsibility. Tactical units maintain smaller sectors of responsibility and are often directly engaged with enemy kinetic forces. Tactical forces are usually younger, composed primarily of enlisted personnel, warrant officers as technical experts, and officers serving as generalist leaders. The

tactical battlefield is often austere, stressful, dirty, with scarce resources, including limited power and network bandwidth. Tactical units are nomadic, reducing the ability to improve their environments. In contrast, operational-level units maintain much larger sectors, often nation-state or larger. Operational headquarters are typically well-developed, fixed locations, and the human dimension includes more senior personnel as well as military, civilian, and foreign representatives from myriad organizations. Strategic headquarters, often located in urban settings, rarely deploy and enjoy easier access to high quality and reliable power, significant bandwidth, and other crucial resources.

A near-future CCOP system may have users trained primarily as kinetic soldiers, with little understanding of cyberspace. The ability to code will initially be uncommon. However, military technologists with cyber warfare expertise will be increasingly common; they will operate CCOP systems and act as intermediaries who translate technical matters for non-technical audiences. Coding skills will thus increase, but some users will possess only general IT and sysadmin-like skill sets. CCOP system products, such as reports, will be consumed by primarily kinetic decision-makers up to the general officer-level, who will likely have minimal technical experience. Military operations rely heavily on skilled planners, primarily trained for kinetic operations, but who will begin receiving training on integration of cyber effects. These planners will increasingly interact with some CCOP systems.

A CCOP's initial success will be a system that addresses operations only in the cyber domain. However, a primary challenge will be how they seamlessly fuse the physical domain with cyberspace for planning and execution of combined arms operations (artillery, infantry, armor, etc.), joint domain operations (ground, air, sea, and space) with both non-expert (kinetic) and expert (cyber specialist) operators and information consumers. For success, the CCOP system must seamlessly interoperate with existing kinetic military command and control systems. This transparent interoperability is crucial for the system's successful employment in a dynamic operating environment.

But what are the cyber responsibilities, operations, and capabilities mandated at each military echelon, particularly at the tactical level? (for early analysis see Grigsby, who advocates combined cyberspace and electronic warfare efforts in support of tactical operations) [19].

B. Task Analysis

A detailed listing of a CCOP's required tasks is beyond this paper's scope. We instead provide an overview of major task areas. At a high level, an *ideal* cyber COP system provides:

- Accurate real-time location (both physical and, where applicable, virtual) and status of cyber and kinetic forces, including friendly, neutral, and adversary.
- The ability to provide machine- and human-based C2 of assigned friendly units throughout ongoing cyber operations.
- Seamlessly integrated displays and processing of information for the air, land, sea, space, and cyber domains.
- Appropriate situational awareness of the environment's tactical, operational, and strategic levels.
- Predictive analysis to anticipate enemy actions and reactions.
- Decision support to help leaders analyze options and make decisions across cyber/physical domain operations.

These objectives are complex and unrealistic in the near term. Many friendly forces, such as special operations forces on covert missions restrict their activities to a closely constrained group. "Need to know" controls on classified information will deny some CCOP users access to important data and create situational awareness gaps. Interoperability issues will frustrate communication between sister services, worse still within multinational coalitions. Adversary forces will actively mask their activities and their intent. Even neutral entities and non-governmental

organizations will not necessarily aid, and may frustrate, tracking their activities. In cyber warfare the entire global Internet is a potential battleground; billions of pieces of electronics are potential combatants. Decision-making will occur in multiple forms based on willingness to accept risk, legal constraints, and operational necessity, including humans in the loop, humans on the loop, and purely machine decision-making [20]. Because of the complexity, initial success means accomplishing *some* of the desired tasks, but built upon an extensible and robust framework to facilitate future expansion. Table 1 provides a high-level overview of potential tasks suitable for a CCOP system [21].

TABLE 1: PARTIAL LIST OF HIGH-LEVEL TASKS FOR AN IDEALIZED CYBER COP SYSTEM

Maintenance	Generate detailed maintenance data suitable for human technicians and automated diagnosis and repair.
Operational Execution	Coordinate highly-complex cyber and kinetic operations; seamlessly allow integration of offense, defense, and exploitation activities.
Electronic Warfare	Integrate electronic warfare capabilities into operations; control friendly and shape enemy electromagnetic spectrum usage.
Forensics	Import insights from forensics systems, capture relevant forensic data from cyber events, and export it to external forensics applications.
Interoperability	Support secure integration and data exchange with a wide variety of systems, including kinetic systems as well as sister-service, multinational, and interagency systems using open and standardized formats.
Targeting	Enable rapid direction of cyber fires despite agile virtual adversaries. Assist with target set development, deconfliction of targets, and the matching of capabilities to desired targets.
Network Analysis	Provide continuous mapping and rapid understanding of the cyber battlespace, including enemy, friendly, and neutral entities, as well as critical nodes. Support study of network bandwidth constraints as being suitable for desired capabilities and to assist in forecasted analyses based on node and link availability. Suggest network paths based on operational needs. Keep pace with cyber maneuver as friendly and enemy operations unfold.
Mission Analysis	Provide support for cyber military decision-making process, including mission analysis, course of action (COA) development, COA analysis (wargaming), COA approval, and orders production.
Mission Rehearsal	Allow operators to rehearse missions, including phasing, sequencing, and timing, and analysis of projected effects.
Battlespace Visualization	Visualize cyber terrain, including large-scale dynamic networks, ideally in real-time, and facilitate delineation of unit sectors of responsibility in the physical and virtual realms.
War Plans	Development of strategic level war plans is beyond the scope of this paper, but automated integration of war plans into a CCOP system will likely be beneficial and a CCOP system may be useful in developing plans perhaps via wargaming or models.
Identify Friend or Foe	Modern kinetic weapon systems use technology to identify whether entities are friendly or enemy; we envision this capability may be possible with cyber platforms.
Battle Damage Assessment	Provide battle damage assessment to analyze forecasted vs. actual effects, including the ability to monitor physical and informational destruction and modification, as well as collateral damage [22]. Provide mechanisms to feedback learning from operations into future planning and prediction sub-systems.

Rules of Engagement	Assist with compliance of authorized rules of engagement, including alerting when approaching legal and ethical boundaries during the planning and execution of cyber operations.
Order of Battle	Monitor the status of friendly, adversary, and neutral order of battle, including irregulars, insurgent groups, criminal organizations, potential insider threats, as well as nation-state organizations along with associated real-world human identities and virtual personas.
Sensor Management	Manage both physical and cyberspace sensors, including issuing of instructions and extracting data.
Training	Possess training and operational modes that allow operators to employ the same system in exercises, simulations, during individual and collective training, as well as operational engagements, supporting the common military practice of "training as one fights."
Capabilities	Provide database of available capabilities and cyber weapon systems, including cost and estimates of risk in usage. System should facilitate integration of new capabilities, awareness of those in use by others, and an ability to remove outdated capabilities from operational consideration. System should suggest candidate capabilities as part of planning process. Integrate notional capabilities for planning and testing purposes.
Weapon System Deployment	Monitor status of cyber weapons platforms and issue commands either manually or via code to automate execution of some stratagems. This goal includes a requirement to synchronize large numbers of cyber weapon systems with millisecond-level precision.
Resiliency and Survivability	Operate effectively despite attack and under degraded network conditions. Provide scalable, reliable, and guaranteed services under all except the most extreme conditions, utilize local caching of data to operate despite network outages, and possess robust backup and failover capabilities, including redundant, load-balanced systems. If the system does fail, it should fail gracefully and securely.
Deception Resistance	Resist human and machine attempts to deceive or otherwise influence decision-making [23]. The system must resist detection despite aggressive threat reconnaissance.
Deception Planning	Provide support for deceptive cyber operations and activities. See the work of O'Connor for examples [24].
Confidentiality, Availability, and Integrity	Operate securely, protect data confidentiality and integrity, and make data broadly available when needed.
Information Operations	Integrate appropriate data from existing information operations systems and planning.
Defensive Operations	Provide comprehensive awareness of friendly networks' health and welfare, including security policy compliance. Appropriately and timely alert human operators of potential and ongoing attacks. Provide shared warning capabilities with allies. Detect, prevent, and respond to attacks and assist with planning and executing counterattacks and adapting defenses. Provide indications of defense failure and recovery activities. When possible identify and isolate attackers (hardware, software, and human). Assist with performing attribution of attacks, despite use of proxies and anonymization.
Intelligence	Assist cyber, SIGINT and all-source analysis. Monitor indicators and warnings relevant to unit's operations. Assist enemy order of battle development, including information on emerging actors, threat signatures, and important cyber events [25]. Fuse information from sensors and intelligence-related cyber missions.
Decision Support	Present options to the commander or operator. Facilitate crosstalk among other friendly decision-makers in the battlespace. Provide decision-support functionality including information from historical and current missions and predictive analysis, including degree of uncertainty, potential risk, desired effects, collateral effects, and legal constraints, for candidate courses of action. Assist in performing intelligence gain-loss calculus. Allow user to display details on the internal logic used by the system.

C. Technology Analysis

Available technology significantly constrains a CCOP's design, particularly at lower echelons. Cloud-based resources can partially decrease the disadvantages of limited resources near the tactical edge. However, cloud resources, while offering the tactical user reach-back capability, are inherently dependent on network connectivity. When networks fail, which is a common battlefield occurrence, a poorly-designed system is effectively useless. Besides, variations in bandwidth and network reliability at each echelon, processing power, display sizes, electrical power sources, and other characteristics vary dramatically (see Table 2).

TABLE 2: TECHNOLOGY TO SUPPORT A CYBER COP SYSTEM VARIES DRAMATICALLY BASED ON MILITARY ECHELON.

	Processing	**Network**	**Interface**	**Power**	**Typical Display Size**
Strategic HQ	High – Extremely High	High	Keyboard Mouse	Reliable, with generator as backup	up to wall size displays.
Operational / Theater HQ	Average	Average	Keyboard, mouse	Generator, possible host nation commercial	up to 60"
Tactical HQ	Modest	Modest bandwidth and possibly intermittent connectivity	Keyboard, mouse	Generator, possibly unreliable commercial	up to 42"
Tactical Vehicle	Limited	Limited bandwidth and intermittent connectivity	Touch, keyboard	Battery, generator	up to 15"
Tactical Individual	Limited	Limited bandwidth and intermittent connectivity	Touch, small keyboard	Battery	3" - 15"

As the table indicates, screen size, processing power, and network capabilities vary dramatically. A CCOP system must account for these aspects. A "one-size-fits-all" solution is unlikely; instead solutions tailored for each echelon, which account for available technical platforms and network resources, will likely be the most promising approach. Despite these differences, similar interfaces, software modules, and interoperable data sources might maximize ease of use and minimize coding and training

requirements. To ameliorate dependence on network connectivity, caching and localized processing can provide resilience against network or other failures.

Some military units embrace innovation and will likely develop prototype solutions. These systems will illuminate promising approaches for future adoption, but will initially frustrate standardization and interoperability. One potential solution is to create an extensible system that actively supports end-user development, such as custom visualizations using the Ozone widget framework, but provided under an overarching standardization framework [26].

Human and technological limitations will constrain the system's visualization aspects. Visual representation of large-scale data remains an open problem since limited pixels populate even the largest display. However, the ability to zoom and filter combined with higher-level analytics, such as attack trees or decision analysis algorithms, can maximize the limited resource of human time and attention. Systems based on formal methods may increase commanders' confidence. Advances in automated analysis and fusion of text, sound, images, video and other sensor data will increasingly enhance capabilities. Gaming and simulation engines may serve as viable frameworks for integration into a CCOP system and are also intimately familiar to computer gamers in the military.

D. Information Flows

A CCOP system relies on its information flows, which can be in a raw form, aggregated, summarized, filtered, anonymized, or combined with other data flows. Transformations might occur upstream, perhaps due to bandwidth constraints, or could occur directly on the system to provide desired insights or prevent user-information overload. However, latency, completeness, and accuracy are constant challenges. Clock drift will cause subtle variations in time-stamped data despite simultaneously occurring events. Data classification will prevent some users from accessing needed information as will data-sharing restrictions among inter- and intra-

national and agency partners, including between privately-owned, civilian, military, and government entities.

Internet data collection is particularly pernicious. The Internet is the operational battlespace, yet simultaneously many CCOP information flows will occur over this same network. Out-of-band communications, such as separate networks for observation and reporting, are expensive, but likely required for critical information flows feeding a CCOP. Importantly, these parallel networks will be high-priority targets and require effective safeguards. As a constantly changing, dynamic system, comprised of billions of computing devices, global, real-time, and comprehensive knowledge of the Internet is an impossibility. The sheer number of states surpasses today's information processing capability and will remain so because increased processing capability spurs the Internet's complexity. However, partial mapping of the Internet's state is possible but time consuming and risky. Packet-based mapping increases detection likelihood and risks unintended impacts on the observed systems, such as crashing a system or triggering automated defenses. Many Internet-connected systems are walled gardens, including social networks and virtual worlds, protected by robust authentication and other means. Others take more extreme measures, creating peer-to-peer distributed networks, which ride over opaque, encrypted channels across the Internet substrate. In these cases, traffic analysis based on message externals may be the only way to garner system information.

The Internet was not designed with attribution in mind. Trust of data should be constantly suspect. Deception is easy and common. Threat, neutral, and friendly forces will mask identities or use traps like honeynets to spoof legitimate systems' characteristics.

Kinetic battlefield and cyberspace sensors are key components of the collection, processing, and dissemination chain. Some information derives from intelligence sources; others arrive from open source intelligence, private industry, and increasingly sensors placed on individual soldiers and weapon systems. Information-sharing agreements are necessary, as are

automated transformations to convert data format. Similarly, automated-language translation will be necessary. Adversary data will always be incomplete or contradictory due to counterintelligence activities. Friendly force data will provide a better but also incomplete picture.

The enduring bandwidth problem can be reduced by fusion, intelligent data filtering, and generation of high-level semantic information flows (e.g. alerts) that disseminate critical information. Bandwidth, link length, and uptime degrades significantly at the network's tactical edge. Expensive and unreliable connectivity will exist under the best of circumstances, and CCOP systems must be partially functional despite loss of or degraded connectivity during a cyber conflict.

CCOP systems require significant interoperability. But military services have historically resisted military-wide interoperability in lieu of service-tailored systems, as have defense contractors, who feel data interoperability threatens vendor lock-in. Designing systems for interoperability will be more efficient than trying to bolt-on post-deployment interoperability. See Sweeney's analysis of Blue Force Tracking (BFT) systems for lessons learned from kinetic systems [27].

E. Interaction

Visualization's power derives through interaction. A key tenet from the information visualization community is Schneiderman's "mantra" : "[O]verview first, zoom and filter, provide details on demand," a common and powerful paradigm oft-employed by the best information visualization systems. Static displays alone undercut a CCOP system's power. Many existing operations centers forego interaction with their large-screen displays, which are too often underused for cable news, UAV feeds, a map or two, or maybe a few Excel-derived bar charts. Today, real work generates from the analyst's desktop. Part of the solution thus requires creating systems that spur individual and team interest and use, rather than visitor "eye candy." We acknowledge, however, that one person's fancy graphics may have value when tailored smartly for senior decision-makers.

The ultimate solution presents data in functional ways, at the strategic, operational, and tactical-level, with user-determined success. The CCOP should help users accomplish tasks quickly and efficiently. The system must map data to a visual display smartly and efficiently. Many resort to Excel-class graphics, but much more intuitive and interactive options are available. The visualization research community regularly generates employable precision visualization and interaction techniques, which represent a powerful, largely-untapped resource. Additionally, empowering users to generate their own visualizations using technologies such as the Ozone widget toolkit mentioned earlier and then create Apple App Store-like environments for community-based sharing may prove useful. We also recommend evaluating the efficacy of the CCOP systems using real-world users in laboratory, training, and operational environments to determine the system's overall impact on task completion, error rate, and speed, as well as developing an understanding of system limitations.

6. Conclusions and Future Work

Constructing an effective cyber common operating picture system remains an elusive but surmountable goal. Deficiencies are inevitable for the foreseeable future. A way forward involves step-by-step research at the intersection of cyberspace with other domains: physical, electromagnetic, information, and cognitive. We should then seek seamless integration of these disparate domains, not just cyberspace. Complete knowledge of even a single domain is unlikely, so future work must focus on developing the sensors, processing systems, and communication networks that provide enough, and the right type of information, at the right time to provide actionable information to support informed decisions by CCOP human and machine users. Throughout this R&D process, user studies based on existing systems must ensure the validity of each candidate solution. Although problematic due to security or competitive concerns, this research data and task analyses derived from studying real-world users should be shared to drive future innovation. Humans, however, are not the complete solution. Whenever possible, we must offload

appropriate work onto machines, allowing humans to focus on work humans can best provide.

Soon we will see candidate CCOP solutions from academia, industry, and from within the military. Now, though, a panacea is highly unlikely—most solutions will merely be evolutionary improvements. Purchasers should be wary of far-reaching claims. However, visualization thoughtfully-designed in a way that complements human and machine strengths while ameliorating their weaknesses, bears great promise. We can learn from the mature kinetic warfighting processes and systems refined over the centuries, as well as from major telecommunication providers, and assimilate their best ideas. Gaps remain, but as we outlined, a viable design process to combine these insights and fill these gaps with new solutions exists. Ultimately, the solution will be iterative, requiring constant evolution based on user-feedback and system evaluation in operational environments far removed from the laboratory. The true success of a CCOP system hinges upon trust, acceptance, and adoption by the operators and decision-makers whom it supports.

REFERENCES:

[1] *JP 1-02 DOD Dictionary of Military and Associated Terms*, U.S. Department of Defense, Oct. 17, 2008.

[2] *FM-3 Operations*, U.S. Army, Feb. 2008.

[3] "Theater Network Operations and Security Center." U.S. CIO/G-6, Architecture Community. Available: http://architecture.army.mil/technical-view/tnosc.html

[4] N. Shachtman. "Darpa Looks to Make Cyberwar Routine with Secret 'Plan X.'" Wired Danger Room Blog, Aug. 21, 2012.

[5] "IBM i2 Analyst's Notebook." International Business Machines Corporation. Available: http://www.i2group.com/us/products/analysis-product-line/ibm-i2-analysts-notebook

[6] A. Vance and B. Stone. "Palantir, the War on Terror's Secret Weapon." Business Week, Nov. 22, 2011.

[7] "Cyber." Palantir Corporation. http://www.palantir.com/solutions/cyber/, last accessed Sep. 17, 2012.

[8] "HP ArcSight Security Intelligence." Hewlett Packard. Available: http://www.hpenterprisesecurity.com/products/hp-arcsight-security-intelligence/

[9] "Product Overview." Splunk corporation. Available: http://www.splunk.com/product

[10] G. Conti. *Security Data Visualization*. San Francisco: No Starch Press, 2007.

[11] R. Marty. *Applied Security Visualization*. New York: Addison Wesley, 2008.

[12] R. Butler, D. Deckro, and J. Weir. "Using Decision Analysis to Increase Commanders' Confidence for Employment of Computer Network Operations." *IO Sphere*, Fall 2005.

[13] C. Steiner. *Automate This: How Algorithms Came to Rule Our World*. New York: Portfolio Hardcover, 2012.

[14] N. Popper. "Searching for a Speed Limit in High-Frequency Trading." The New York Times, Sep. 8 2012.

[15] D. Ford. "A Vision So Noble: John Boyd, the OODA Loop, and America's War on Terror." Create Space, 2010.

[16] M. Miller, J. Brickey, and G. Conti. "Why Your Intuition About Cyber Warfare is Probably Wrong." *Small Wars Journal*, Nov. 29, 2012.

[17] This paragraph draws heavily upon the U.S. Army's five paragraph operations order format.

[18] C. Clausewitz, *On War*. USA: Empire Books, 2011.

[19] W. Grigsby, G. Howard, T. McNeill, and G. Buehler. "CEMA: A Key to Success in Unified Land Operations." *Army*, Jun. 2012, pp. 43-46.

[20] P. Hew and E. Lewis. "Situation Awareness for Supervisory Control: Two Fratricide Cases Revisited." International Command Control Research and Technology Symposium, 2010.

[21] A complete cataloging of tasks is far beyond the scope of this paper, but we suggest studying the "The National Cybersecurity Workforce Framework" developed by the U.S. National Institute of Standards and Technology (NIST). Available: http://csrc.nist.gov/nice/framework/

[22] R. Fanelli and G. Conti. "A Methodology for Cyber Operations Targeting and Control of Collateral Damage in the Context of Lawful Armed Conflict." International Conference on Cyber Conflict (CyCon), Tallinn Estonia, Jun. 2012.

[23] G. Conti, M. Ahamad and J. Stasko. "Attacking Information Visualization System Usability: Overloading and Deceiving the Human." Symposium on Usable Privacy and Security, Jul. 2005.

[24] T. O'Connor. "About Face: Defending Your Organization Against Penetration Testing Teams." SANS Information Reading Room, Dec. 2010.

[25] "Department of Defense Strategy for Operating in Cyberspace." U.S. Department of Defense, Jul. 2011.

[26] "Ozone/Synapse Download Portal." Potomac Fusion. Available: http://widget.potomacfusion.com/main/home

[27] M. Sweeney, "Blue Force Tracking: Building a Joint Capability," U.S. Army War College, Mar. 15, 2008.