Lifting the Interagency Fog of Information:

Blockchain Information-Sharing and Radical Inclusion

by Jaymes "Yuri" Hines and Mark A. Williams

The fog of information can drive out knowledge.

–Daniel J .Boorstin

In "Radical Inclusion," General Martin Dempsey and Ori Brafman offer current and aspiring leaders extraordinary insights into getting the best possible information for decision making as well as how to rely on trust and participation to forge strong teams."

–Robert M. Gates

Eureka!

The authors of this piece began an adventure into information-sharing. It was a eureka moment of "hey, let's talk about the challenges to information-sharing and use West Africa as a vehicle to explore information-sharing and its associated challenges." The task seemed daunting, a struggle to form ideas about employing blockchain technology to facilitate interagency information-sharing.

The emergence of two seemingly-independent ideas formed into a cogent awareness of the necessity of combining blockchain technology with sweeping information-leadership concepts put forth in the book *Radical Inclusion* by General (retired) Martin Dempsey and Ori Brafman. Blockchain technology holds the potential to assure total access to information, while simultaneously enhancing information security. A brief review of literature demonstrates that governments and agencies are investigating the use of blockchain technology as a solution to the myriad of information

Major Jaymes "Yuri" Hines, U.S. Air Force, is a Combat Search and Rescue Pilot who assists the Assistant Secretary of the Air Force with overseeing the Air Force's Warrior Wellness and Policy Integration. He holds a Master of Aviation Science from Embry Riddle University and a Master of Military of Military Art and Science degree in Strategic Studies from the U.S. Army Command and General Staff College.

Major Mark A. Williams, U.S. Air Force, is the Director of Operations at the 132nd Intelligence, Surveillance and Reconnaissance Group, Iowa Air National Guard. He is a prior logistics officer and has published work in the Exceptional Release, a logistics magazine. Mark holds a Master of Military Art and Science degree in Strategic Studies from the U.S. Army Command and General Staff College where he is also a graduate of the West Africa Scholars Program.

dilemmas. And sweeping information-leadership concepts were the subject of a recent symposium hosted by the U.S. Army's Command and General Staff Officer's Course that discussed the conceptual foundations of the book, including the rise of the digital echo, the dissention of fact and narrative, and the subsequent impact on effective leadership. While *Radical Inclusion* discussed the role of leadership in a new information environment, the concepts are easily applied to radical solutions to information-sharing in the interagency and multinational context. To this end, this article combines the concepts of the digital echo and radical inclusion to leverage blockchain technologies as the interagency information-sharing standard of the future.

This article is organized to provide the reader with a proof of concept grounded in a historical precedent that highlights the failures and successes of an interagency information-sharing operation. The vehicle for incorporating these elements into a discussion of an interagency information-sharing case study is driven by a case study on the 2013 Ebola Virus Disease outbreak and crisis in West Africa. In that noble pursuit, this article explores the multifaceted challenges with interagency information-sharing, contextualized within the U.S.'s response to the outbreak. This article provides insight into the exigent barriers, risks, and opportunities of information-sharing across agencies, organizations, governments, and nongovernmental organizations. In doing so, illuminating and addressing existing challenges to information-sharing sets the stage for advancing blockchain technology as a mechanism for total and secure information-sharing across agencies. While blockchain technology provides an apparatus for total and secure information-sharing, it only represents one cog within the total system of information-sharing. To address this issue holistically, one must also address institutional information-sharing policies, as well as consider the human aspect of sharing and trusting information. The strategic and operational intersections of these elements lead to an operational approach that evaluates and operationalizes each component. This approach incorporates three distinct lines of effort: the technical system, the institutional system, and the human system.

Before discussing these lines of effort, as well as the barriers and risks to such efforts, this article provides an interagency information-sharing scene setter, the 2013 West Africa Ebola outbreak and subsequent interagency and multinational responses. Equal in the significance of the political, human, and economic impacts of the outbreak and response are the implications toward the existing challenges of information-sharing, challenges often characterized as contributing to the "fog of information."

The fog of information... is a metaphor describing a lack of data that obscures situational awareness and inhibits decision-making.

The Fog of Information

The fog of information is rapidly becoming a truism of information-sharing. It is a metaphor describing a lack of data that obscures situational awareness and inhibits decision-making. In some form or fashion, as a reader, you have been either a contributor to or on the receiving end of the fog of information. Personifying the phrase, one can imagine trying to make decisions with partial data, no data, or an overload of data. According to Daniel Boorstin, "the fog of information can drive out knowledge." The reality is that the fog exists as a blinder to information awareness—the awareness and synthesis of information. The fog of information affects the strategic, operational, and tactical levels of planning. It can be created by environmental conditions, operational limitations, and may often be self-

induced. In all cases, the result remains constant, the fog of information is a limitation in the total and secure access to, dissemination of, and reception of information. It is a malignant outcome of ineffective information-sharing mechanisms, processes, and policies. The fog of information is persistent; it has existed in multiple interagency antecedents and was highlighted in the assessment of the interagency response to the 2013 West Africa Ebola crisis response.

The Fog of Information Settles: The Interagency Response to the Ebola Crisis and Lessons Learned

The 2013 outbreak of the Ebola virus devastated the West Africa region ending in more than 28,600 confirmed cases and 11,325 deaths in multiple countries.[1] The U.S. response to the humanitarian crisis involved U.S. agencies in coordination with nongovernmental organizations. The Obama administration described the U.S. response as a "whole of government approach."[2] The U.S. committed specialists from multiple departments and agencies, including the Departments of State, Defense (DoD) (through Africa Command [AFRICOM]), and Health and Human Services (HHS); the Centers for Disease Control and Prevention (CDC); National Institutes of Health (NIH); and U.S. Agency for International Development (USAID).[3] Moreover, the scale of the response was global, equal in its significance to the threat of non-containment. The United Nations (UN), African Union (AU), World Health Organization (WHO), foreign governments, and other partners contributed resources. In total, the Ebola response included multiple stakeholders, and the unity of effort spanned international organizations, companies, bilateral donors, regional organizations, national governments, nongovernmental organizations, local communities, and individuals.[4]

The failure of sharing information, for whatever reason, may result in the failure of operationalizing the strategy.

The U.S. strategy to combating the Ebola crisis centered on four key goals: 1) controlling the epidemic at its source in West Africa, 2) mitigating second-order impacts, including blunting the economic, social, and political tolls in the region, 3) engaging and coordinating with a broader global audience, and 4) fortifying global health security infrastructure in the region and beyond.[5] True to form, the U.S. committed over 175 million dollars within the year. However, any effective strategy tailored to an end state must conceptualize and disseminate information that describes the operating environment, designates the various environmental and mission variables, and, ultimately, shares information across networks to the involved agencies and departments. In this regard, the strategy typifies the whole of government approach. Such an approach is characterized as an interagency approach. The failure of sharing information, for whatever reason, may result in the failure of operationalizing the strategy.

Following the initial Ebola crisis response in 2013 and 2014, the U.S. government came together with other nations to launch the Global Health Security Agenda (GHSA) as a multiyear effort to increase global health security and response capacities and capabilities. A cornerstone to this effort is the commitment toward build information systems that increase the ability of the international community to respond to future humanitarian crises. Multiple studies stemming from this effort considered the lessons learned with respect to coordinating international responses to such crises, strengthening health systems, and improving related tools and procedures. Inherent within that effort is reframing how the interagency and international communities adapt and adopt

these lessons. Drawing on the Ebola outbreak experience, this article briefly synthesizes two such studies to build a conceptual framework for an operational approach. Furthermore, a review of the literature regarding information-sharing within the Ebola response substantiates a call for action for addressing systemic challenges of interagency information-sharing.

The U.K.-based Save the Children Organization study "Ebola: Lessons Learned" illuminates shortfalls to the existing information systems in the West African regions of Liberia, Sierra Leone, and Guinea. The study found that these countries lacked basic functioning information systems, which led to a diminished ability to access and analyze data and information critical to planners, responders, and decisionmakers.[6]Accordingly, a lack of a distributed information system that provided total and secure access to information and data prevented the efficacy of the interagency and multinational response. Of the health information systems available within the West Africa region, most were stove-piped, disconnected, and fragmented below the national level.[7] While this study presents the failures of information-sharing within the larger context of failing health systems, the implications for interagency information-sharing are easy to draw. Fundamentally, as a regional health system within Liberia, Sierra Leone, and Guinea, the access to and sharing of information was detrimental to the recovery efforts. As the world responded (including the U.S. interagency system), the efforts to share information would struggle due to the diminished information-sharing systems within the West Africa Region. A 2013 USAID study, "Fighting Ebola with Information: Learning from Data and Information Flows in the West Africa Ebola Response," further discusses the international community's response and provides additional lessons learned.

The USAID study focuses specifically on the multifaceted response and the role of data and digital technologies. This study makes multiple characterizations regarding information-sharing. The study addressed three primary questions:

1. What contributed to the "fog of information" that characterized so much of the early stages of the Ebola outbreak response?

2. What can be learned from the use of data, information, and digital technologies during the Ebola outbreak response? How and where were they used effectively?

3. What should be done to improve the use of data, information, and digital technologies in the emergency contexts to support long-term recovery and to build resilience against future shocks?[8]

Of the health information systems available within the West Africa region, most were stove-piped, disconnected, and fragmented below the national level.

In answering these questions, the USAID study distills the factors that form the fog of information into three sub-systems within the context of the larger information-sharing system employed during the Ebola crisis response. The study characterized the fog of information as "the lack of timely, accurate, and accessible data, which clouded situational awareness, impeded effective decision-making, and stymied the response."[9] Regarding questions two and three, the summation of the study's findings is best represented in the following quote: "Information was critical to the fight against Ebola. Both for responders [and agencies], who needed detailed and timely data about the disease's spread, and for communities, who needed access to *trusted* and *truthful* information with which they could protect themselves and their loved ones."[10] Further, the study advances that strengthening

the technical, institutional, and human systems within the larger context of information-sharing systems requires the ability to rapidly gather, transmit, analyze, use, and share data.[11]

The USAID report presents eight recommendations for reforming the information-sharing system utilized by the interagency response to the Ebola crisis:

1. Recognize and identify information as a valuable commodity for preparedness, response, and resilience.

2. Invest in the infrastructure required for digital connectivity, as elements of preparedness, response, and resilience.

3. Invest in workforce and institutional capacity and in the enabling and regulatory environments to enable and capture the full value of real-time or near real-time information flows.

4. Advance harmonized data standards and interoperability guidelines and practice to enable data systems to "speak to" one another.

5. Coordinate investments in digital health programs to avoid duplication and fragmentation.

6. Build capacity to design and deliver digitally-supported programs in a way that adheres to best practice, such as that embodied in the Principles for Digital Development.

7. Leverage the lowered barriers of access to communications to more regularly engage nontraditional actors, such as citizens, frontline workers, and remote responders, in health and aid programming design, delivery, and evaluation.

8. Use real-time or near-real time data and information flows to incorporate feedback and insights from localized data collection to adapt and improve programming and to create the opportunity to devolve decision-making to the point of data collection.[12]

The study concludes that strengthened data and information flow presents an opportunity to reform interagency processes and programs such as health and humanitarian aid. It acknowledges that this transformation will require a vision for change and a plan for implementation.[13]

The U.S. Blockchain Forum

The 2017 U.S. Forum on Blockchain Technology was a consortium of agencies advocating for and advancing concepts of blockchain information-sharing. Specifically, the interagency forum met to "learn about advances in Blockchain technology, discuss use cases and set an agenda for working together to evaluate and implement it among our diverse missions."[14] this forum represents a call for action regarding reform, vision for change, and implementing a plan for action. Sixty agencies and departments from the U.S. government (including USAID, DoD, and State) met to discuss case and concept proposals for the inculcation of blockchain technology for the interagency information-sharing process.[15]

The Ebola response studies highlight significant challenges currently existing within the interagency information-sharing system. The USAID study broke down the West Africa interagency information-sharing system into three distinct subsystems. The subsystems include technical, institutional, and human systems, and each contains its respective challenges and barriers toward total and secure information-sharing. However, each system also provides a foundation for opportunities of holistic information-sharing improvements. Transformative change within these systems requires leadership, vision, and a plan of action. The U.S. Forum on Blockchain Technology set

a vision and plan of action in place to leverage blockchain technology among agencies and departments within the government. This article presents a step-forward in that direction by operationalizing the three sub-systems of information (technical, institutional, and human) into three lines of effort to transform the current model of interagency information-sharing.[16] It articulates these lines of effort against the backdrop of the interagency and multinational response to the 2013 Ebola outbreak and crisis response.

Collectively, combining a distributed information-sharing system, employed through a blockchain architecture leverages timely, tailored, and effective information-sharing that promotes synchronized cooperation between interagency and multinational efforts. The first line of effort, the technical system, proposes blockchain technology as an enhanced security and validation tool, as well as a forum for open and total information-sharing among stakeholders. The second line of effort, the institutional system, advances both collaborative and inclusive approaches to interagency information-sharing. However, certain statutes and policy must be introduced or reformed to maximize the utility of such an approach. As such, employing blockchain technology will require a holistic reinvigoration of information-sharing capabilities and reform of interagency information-sharing policies. The third line of effort, the human system, incorporates concepts of radical inclusion and addresses the question, "How do we create an inclusive approach that frames truth in terms of context and narrative?" This line of effort seeks to establish a framework that provides for enhanced mutual trust among information stakeholders.

Technical System

For the first time in human history, people anywhere can trust each other and transact within large peer-to-peer networks without centralized management.[17] Trust is established not by centralized institutions but by protocols, cryptography, and computer code.[18]

The application of these modalities of digital information-sharing greatly strengthens the capacity for cooperation and collaboration between organizations and individuals within peer networks. The implication being that global networks of collaboration without centralized formal institutions will increase the instantaneous and assured access to trusted digital information. This unprecedented, yet increasingly relevant mass collaboration data-exchange is a singular characteristic within the age of globalization, as a response to twenty-first century challenges.

Blockchain is a complex technological, economic, and social phenomenon calling into question commonly-accepted parameters of value, trust, and exchange.

Blockchain is a complex technological, economic, and social phenomenon calling into question commonly-accepted parameters of value, trust, and exchange. The technology creates a trust machine that enables transparency and collaboration, two stalwarts of the rapid transformation of the culture within the information-sharing community. As mentioned, the structure is neither centralized nor decentralized but a distributed network.

The strength of the blockchain information system is the distributed user interface. Such a system allows for a community approach to ensuring trust, reliability, and validity of information flow. This way no one partner could "cheat the system" by editing records because everyone using the system would be watching. Systems like this are on the horizon, and the software that powers them is called a blockchain. Blockchains store information across a network of designated computers. Making them not

just decentralized but distributed. This means no central nation or user owns the system, yet everyone can use it or help run it. This is important because it means it is difficult for any one person to take down the network or corrupt it. The blockchain uses a form of math called cryptography to ensure that records cannot be counterfeited or changed by anyone else. Blockchains that manage and verify online data could enable us to launch networks that are entirely run by algorithms helping us protect online identities. In this manner, information and intelligence is factual, accurate, and secure, verified by anyone within the system.

The blockchain uses a form of math called cryptography to ensure that records cannot be counterfeited or changed by anyone else.

The setup process is critical to effectively implement the technological advances of blockchain. First, identify the stakeholders of an event, operation, crisis, and pandemic. These stakeholders may include AFRICOM, the European Union, the UN, the US, and any one or all nation-states within the African Region. It may include two or more stakeholders for cooperation, collaboration, and the sharing or exchanging of information.

Second, identify the event the stakeholders will be participating in. Blockchain allows the actors in an armed conflict or any scenario to have the situation broken down into a network of separate conflicts and/or bilateral relationships among the parties. Each of these relations can then be qualified. These events may include counterterrorism; a military operation; natural disaster response, such as earthquakes, hurricanes, volcanoes etc.; and pandemics, such as the Ebola response case study discussed in this article. Because blockchain technology is so robust and advanced, there can be several events within the forum, and several different stakeholders will have access capability to the events deemed necessary.

Third, there must be a trust protocol criterion established that allows the different stakeholders to access the technology and share information. Creating an application criterion to gain access ensures that the correct stakeholders have access to the correct forums, scenarios, or information. The trust protocol also ensures protection of the established network, and that only interested parties have access. Stakeholders will then have access to the system through an encrypted gate that also prevents unwanted cyberattacks or attempts to attack the architecture; however, due to the technology, this is virtually impossible.

Finally, inside of the architecture, stakeholders will have access to streams of information based on the event accessed. These streams have input capabilities to both read and compose information. What makes blockchain successful is the validation process for a transaction. The technology incorporates a validation process, similar to the already existing transaction confirmation process, which allows all users to validate shared information or pieces of information based on their own information gathering efforts. The information statement once validated, continues to gain or show strength based on the number of confirmations it receives from the interested parties. Since a financial transaction must be validated in several (sometimes up to seven) different locations in order to cement the transaction in the ledger, sharing information can be done similarly. Except, the validation happens when the different users validate that piece of information giving it strength. A shared portion of information with seven validations may appear stronger than a shared portion of information with only two validations. This will address trust and make the users feel at ease with the use of this intelligence/information because it has essentially been confirmed by several entities.

It is common knowledge that information suffers from an inconsistency; it is only valuable when shared with those who need or can benefit from it. However, the more it is shared, the more it risks being compromised. On this platform, these information-sharing relationships are embedded in a larger bilateral relationship, which might involve alliances, military cooperation, and economic cooperation. This platform could mitigate some of the consequences in the event of a crisis and presents the partners the opportunity and ability to share relevant information quickly and safely.

If you cannot trust your partners to treat the information you share in some secure fashion, then there is a major cost for the sharing or the sending state. Information is a commodity, and states share out of mutual interest or to extract things such as foreign aid and security assurances. The providers of information cannot be sure that the receivers will adequately protect what they receive, and the receivers cannot be sure of the veracity of the information provided. This process should not seem like spontaneous sharing, which could be very troubling to other countries because that it is so unpredictable.

Institutional System

The success of a multinational operation hinges on timely and accurate information-sharing. The development of a culture of trust, rooted in an effective information-sharing environment, ensures that all parties within the information-sharing environment can weigh the best available intelligence when developing a course of action. Agencies and stakeholders should begin developing information products with a multinational focus from the beginning of an operation. Using guidance from appropriate regulatory and reference documents and coordinating with a foreign disclosure officer can empower multinational partners to utilize the information and drive operations.

The advocacy of this line of effort acknowledges the existence of and necessary reform to information-sharing barriers such as policy and status. For example, the use of classification, whether U.S. classifications or alliance, such as NATO, classifications impose restrictions on information-sharing, dissemination, and fusion of information products. Too often, however, partners fail to share information because they lack an understanding of classification requirements, caveats, and/or over-classification. As a way forward, blockchain technologies may foster the development of new information-sharing standards, break-down the asymmetric relationships, and, ultimately, create an international regime of information-sharing and a global forum for collaboration between trusted partners. In either case, the adjudication of and reform of existing legacy policies must be a first step, as suggested in the U.S. Forum of Blockchain Technology. However, the implications of blockchain technology are not simply focused on interagency applications, considerations for multilateral information-sharing is also considered.

Too often, however, partners fail to share information because they lack an understanding of classification requirements, caveats, and/or over-classification.

"A multilateral agreement is an accord among three or more parties, agencies or national governments."[19]Accordingly, multilateral information can be similar to intelligence, but the writers have adopted the word information to avoid the additional pitfalls that the sharing of intelligence creates. However, this article employs a similar definition for information which is "the collection, protection, and analysis of both publicly available and secret information, with the goal of reducing decision

makers' uncertainty about a foreign policy problem or issue."[20] The Oxford Dictionary defines collaboration as "the action of working with someone to produce something." So multinational information-sharing for the purpose of this argument, is an accord among two or more agencies or national governments working together to collect, protect, and analyze information to reduce decision makers uncertainty about a foreign policy.

Radical inclusion is a prescription to conquer the fear of losing control...

Human System

The human system line of effort centers around a central construct: "How do we create an inclusive approach toward employing blockchain information-sharing that frames information-truth in terms of context and narrative?" Unequivocally, the center of gravity for this line of effort is people. Therefore, this line of effort seeks to establish common principles, imbedded in interagency leadership competencies that establish a framework of enhanced mutual trust among the people who are the information stakeholders. These stakeholders are organized into the leaders and followers who are involved in information-sharing processes. Collectively, the people involved in the interagency information-sharing process will require dynamic leadership that promotes unfettered and inclusive collaboration and cooperation.

In the book, *Radical Inclusion*, General (retired) Martin Dempsey and Ori Brafman describe the contemporary operating environment as a digital echo. The era of the digital echo results from the speed and ubiquitous dissemination of and access to information. It is a neutral force that informs, misinforms, educates, entertains, and inspires. In this manner, it is a leadership challenge and a leadership opportunity.[21] Furthermore, the combination of these aspects of information-sharing creates vulnerabilities toward the sharing of factual information and may erode the trust between leaders and followers, as well as the information stakeholders.[22]

To mitigate the challenges and exploit the opportunities within the era of the digital echo, information-sharing must incorporate the concept of radical inclusion. Radical inclusion is a prescription to conquer the fear of losing control in the fast-paced, complex, and highly-scrutinized environment that is pushing agencies and governments to rely on philosophies of exclusion. The information-sharing approach advocated for in this article will require a foundation of instinctual inclusion, whereby information and data sources are openly accepted and equally scrutinized. The human system will, in the intermediate, rely on the adage of "trust but verify." Humans will need to remain in the loop in the information-sharing systems. However, as the benefits of artificial intelligence continue to permeate information-sharing systems, the principles of trust, verification, and reliability may shorten the information-sharing timeline and further amplify the benefits of interagency blockchain information-sharing modalities.

As the U.S. incorporates blockchain technology, the assured access to and analysis of information will illuminate new challenges and opportunities. Interagency collaboration and cooperation will require more attention, more learning, more effort, and more inclusion.[23] Ultimately, blockchain technology provides for assured access to the diversity of real-time or near real-time information. In this manner, leaders and stakeholders may become increasingly exposed to raw data that competes to expose truth. The primacy of competing narratives will dominate the decisionmaker. A strength of block-chain technology is its inherent ability to control verified information.

Regardless, the decisionmaker must understand that a philosophy of inclusion—assessing multiple sources, as fringe as they may seem, will leverage a diversity of sources to build a picture of reality (sense-making) through factual information to create a common operating picture and permit organizations and governments to create a "winning narrative."[24]

The human system should be grounded within the leadership theories presented in *Radical Inclusion*. This article combines the concepts of the digital echo and radical inclusion as a human element. Their symbiotic relationship leverages blockchain technologies as the interagency information-sharing standard of the future. The human system will rely on the technical and institutional systems and vice versa. The transformative change to interagency information-sharing demands this inclusive approach. Inclusion, in this manner, not only supports the integrated lines of effort toward information-sharing, it also unlocks understanding and opportunity for leaders and information stake holders.[25]

The Fog Lifted: Operationalizing the Lines of Effort within the Ebola Crisis Response

As with any case study evaluating new concepts within a historical context, some imagination is required. Yet a case study of the 2013 interagency and multinational response provides a framework for applying the lines of effort as an operational approach.

The technical system.

The value proposition for integrating digital technologies lies in enabling a richer, more diverse, and rapid data and information exchange. The benefits to such an open exchange approach apply to interagency health and humanitarian programs, particularly in crisis response operations (such as the Ebola outbreak and ensuing response),[26] which includes the following:

1. Increased accountability, insights, and incentives.
2. An ability to create feedback loops through the sharing of contextualized data and information back to the point of origin.
3. An ability to validate information among stakeholders to ensure leaders can provide timely and accurate decisions.
4. The ability to implement continuous learning and adaptive programming, in which activities are modified and, ideally, regularly adapted in real-time or near real-time data and information.
5. The ability to make better-informed decisions at all levels.[27]

Ultimately the goal is to strengthen the use of digital data and information flows in emergency contexts to support long-term recovery and to build resilience against future shocks like the recent Ebola outbreak in West Africa.

...a blockchain system of information-sharing would have provided a common user platform for open and secure information exchange.

Within the context of the interagency and international response to the Ebola outbreak, a blockchain system of information-sharing would have provided a common user platform for open and secure information exchange. Agencies and organizations such as AFRICOM, UN, EU, USAID, AU, and WHO would comprise the user interface. The distributed information network would rely on the common architecture of assured information flow. The "gated access" node comprised of the trust protocol and access barrier exists as a single point of entry barrier. The benefit of this approach creates a single-

entry barrier rather than the multiple entry and access barriers currently present on the multitude of information systems. The information flow targeted to health and humanitarian responses include data acquisition, storage, and retrieval systems for the Ebola virus allowing for improved accuracy of individualized patient data and disease trajectories. At the community and individual levels, agencies enjoy instantaneous prognostic and diagnostic determinations for patients experiencing symptoms.

The distributed network technology allows for the immediate and redundant validation of information.

The distributed network technology allows for the immediate and redundant validation of information. Picture a spreadsheet that can be duplicated several or even a thousand times across a network. Again, because no centralized version exists, it cannot be hacked, which also creates transparence as well as being incorruptible. It is transparent because it is embedded within the network, but available to users who have gained access. The validation creates trust and strengthens the information shared. For example, during the Ebola crisis, organizations would not have the same confirmation of the known number of cases during the outbreak, which created trust issues with the local population. With the validation process of blockchain technology, a piece of information gains strength each time another partner or shared-stakeholder confirms that piece of information. An organization confirming 21 cases of Ebola in a region could be confirmed when another organization confirms those cases. If the additional organization claimed 27 cases, the first 21 confirmed cases gains strength with a potential of 6 more cases in that region waiting to be confirmed. This concept holds true with any type of information shared, making the validation portion of the blockchain technology very relevant.

The Institutional System

This line of effort focuses on two key components: 1) appropriate classification of information, and 2) analysis of what national and agency systems are in place to handle information and data, measured against the commonality and accessibility of such systems. The Ebola response was a multinational effort, spearheaded by various interagency, governmental, and nongovernmental organizations. Therefore, the information-sharing network must exist within a multinational and interagency context. Here again, the appropriate policy definition of information-sharing should be, "an accord among two or more agencies or national governments working together to collect, protect, and analyze information to reduce decisionmakers' uncertainty about a foreign policy." Operationalizing this definition into policy and statute promotes appropriate classification of information, as well as the employment of a blockchain network tailored to the governments and agencies responding to the outbreak. While this article does not advocate for a specific example, the common principle of information-sharing should be grounded in the philosophy of assured access. Any successful future operation demands such an institutional approach.

The Human System

The wedding of the concepts between blockchain and radical inclusion seemed only natural to the authors. Presenting an argument that advocates for this symbiotic relationship seemed challenging at first. The third line of effort toward implementing the distributed information-sharing system known as blockchain sharing involves the human system. The concepts within this line of effort, as applied to the Ebola response case study combine the unique attributes of radical inclusion. Specifically, the

concepts of information-leadership. Perhaps the most effective way to present this line of effort is through a traditional hypothesis: "If the interagency approach toward information sharing merges blockchain technology and legislation that takes advantage of this technology; the human system must also undergo a radical alteration."[28]At first, this hypothesis seemed amorphous; however, the conclusions from the USAID study provide a pseudo-empirical basis for advancing this argument. The concepts of the human system are integrated into a proposal for operationalizing this line of effort within the context of the interagency response to the Ebola crisis.

Of the eight recommendations proposed by the USAID's Fighting Ebola with Information study and the 79 potential use cases presented from the U.S. Federal Blockchain Forum, the human system line of effort capitalizes on several of these recommendations and proposals. Leaders and information stakeholders within an assured-access, blockchain-enabled, information-sharing environment must understand the digital echo and apply inclusive leadership processes and competencies. The USAID approach leverages the lowered barriers of access to communications to more regularly engage nontraditional actors, such as citizens, frontline workers, and remote responders, in health and aid programming design, delivery, and evaluation.[29]Additionally, employing this human system line of effort maximizes information-sharing as a valuable commodity for disaster and crisis response and resilience. The U.S. Federal Blockchain Forum's potential use cases closely align with the human system approach. Inclusive information-sharing approaches promote security with documentation and data sharing, authentication, and validation of government data; enable coordination and cooperation between federal governments; and ensure security and audit ability when moving information across blockchain systems.[30]

Risks[31]

The increasing ubiquity of blockchain technology is calling into consideration its potential across domains and government sectors. However, the advances in employing blockchain within information-sharing systems present significant risks. Yet, these risks are not entirely new, nor is the prerequisite requirement of trust. Recall the human system adage, "Trust but verify." No matter the relationship, nations rely on a combination of trust among users and built-in institutions that verify information.

...the advances in employing blockchain within information-sharing systems present significant risks. Yet, these risks are not entirely new, nor is the prerequisite requirement of trust.

Governments, departments, and agencies may be cautious about sharing sensitive information for several reasons, whether to protect their own interests or because they are wary about disclosing sources and methods. Also, there is inherent risk that other countries may try to figure out the sources and methods that the sharing country used—reverse engineering of information. There is also worry about the reliability of foreign information, especially if another country has a limited way to independently assess the truthfulness of the shared information. An information-sharing country may have poor collection protocols or "shade" the information to influence local or international policy.

Both preventing the sharing of information (especially when the information can assist partners or sovereign nations from risky situations) and spontaneously disclosing sensitive information can break the bonds of trust among partners, as either of these scenarios may be seen as a betrayal of an information-

sharing agreement. However, partners may also feel the need to view the situation in the context of furthering other interests.

Conclusions

Perhaps Deputy Secretary of State John J. Sullivan said it best in his 2017 opening remarks at the U.S. Federal Blockchain Forum when he stated, "Blockchain technology is not a panacea; it's not the answer to every problem. But we're certainly hopeful that the State Department and the federal government can leverage this technology to make us more efficient and better able to serve the American People."[32] Operationalizing the recommended lines of approach will not only incorporate advanced technologies, such as blockchain information-sharing systems, it will also reform and introduce appropriate policy and statutes that leverage the assured access to and dissemination of real-time credible information-sharing. Ultimately, this operational approach depends on the human system. Comprised of leaders and followers as well as information stakeholders, this approach requires a foundation of radical inclusion leadership competencies that permeate and promote inclusive sharing, security, and utilization of interagency information-sharing. Interagency and multinational information-sharing relies on mutual trust to accomplish objectives and achieve end states. Ultimately, the goal of this information-sharing approach influences the decisionmakers' and stakeholders' ability to assess the environment with the potential of achieving these objectives. Within West Africa, the multinational and interagency efforts that have traditionally struggled under the strain of traditional information-sharing models require a reinvigorated approach to information-sharing—a step forward we have taken together, the next step is up to you. ***IAJ***

NOTES

1 The Centers for Disease Control and Prevention (CDC), "2014-2016 Ebola Outbreak in West Africa," <https://www.cdc.gov/vhf/ebola/history/2014-2016-outbreak/index.html>, accessed on June 1, 2018.

2 The White House, Office of the Press Secretary, "FACT SHEET: U.S. Response to the Ebola Epidemic in West Africa," <https://obamawhitehouse.archives.gov/the-press-office/2014/09/16/fact-sheet-us-response-ebola-epidemic-west-africa>, accessed on June 1, 2018.

3 Ibid.

4 Larissa Fast and Adele Waugaman, *Fighting Ebola with Information: Learning from Data and Information Flows in the West Africa Ebola Response*, United States Agency for International Development, Washington, D.C., 2016.

5 FACT SHEET: U.S. Response to the Ebola Epidemic in West Africa."

6 Simon Wright et al., "A Wake-up Call: Lessons from Ebola for the World's Health Systems," Save the Children, London, UK, 2015, p. 5, <https://www.savethechildren.org.uk/content /dam/global/reports/.../a-wake-up-call.pdf>, accessed on June 1, 2018.

7 Ibid.

8 Fast and Waugaman, p. 9.

9 Ibid., p. 120. "Fog of information" is a variation of the term "fog of war," first attributed to the

Prussian military strategist Carl von Clausewitz. The phrase incorporates many elements including the difficulties of decision-making amid conflict when full situational awareness is often absent.

10 Ibid., p. 7.

11 Ibid.

12 Ibid., p. 119.

13 Ibid.

14 U.S. Federal Blockchain Forum, *U.S. Emerging Citizen Technology Atlas*, 2017, <https://emerging.digital.gov/blockchain-forum/>, accessed on May 23, 2018, p. 3.

15 Ibid. The U.S. Federal Blockchain Forum, hosted on July 18, 2017, brought together executives from various agencies across the federal government to learn about advances in blockchain technology, discuss use cases, and set an agenda for working together to evaluate and implement it among diverse missions. These rough draft use cases represent initial ideas and moonshots as well as programs in development and should be considered only proposed use cases and concepts unless otherwise noted.

16 This article incorporates the USAID studies' components of information sharing (technical, institutional, and human) as sub-systems to the larger interagency information-sharing system that was employed during the 2013–2016 Ebola crisis response in West Africa.

17 Complexity Labs, *Rethinking Economics in an Age of Networks*, <http://complexitylabs.io/>, accessed on June 4, 2018.

18 Ibid.

19 Business Dictionary, multilateral agreement definitions, <http://www.businessdictionary .com/definition. multilateralagreement.html>, June 2, 2018.

20 James Igoe Walsh, *The International Politics of Intelligence Sharing*, Columbia University Press, NY, 2010, p. 5.

21 Martin Dempsey and Ori Brafman, *Radical Inclusion: What the Post 9/11 World Should Have Taught Us About Leadership,* Missionday Publishing, Virginia, 2018, p. xiii.

22 Ibid.

23 Ibid., p. 171.

24 Ibid., p. 14. The authors state, "Despite our best efforts, there will still be times when truth cannot be reliably distinguished from fiction. In the absence of verifiable truth, competing narratives will view for allegiance. When we are forced to compete in a battle of narratives, inclusion is still our best weapon: only by leveraging a diversity of voices can we create a winning narrative."

25 Ibid., p. 167.

26 Fast and Waugaman, p. 9.

27 Ibid.

28 2017 U.S. Federal Blockchain Forum, July 18, 2017, <https://emerging.digital.gov /blockchain-forum/>, accessed on January 5, 2019. This interagency forum, hosted at the General Services Administration, was for executives across the federal government to learn about advances in Blockchain

technology, discuss use cases, and set an agenda for working together to evaluate and implement it among our diverse missions. Use cases represent initial ideas and moonshots as well as program in development. Potential Use Case Observation 35 states: "Improve Local Level Community Engagement, Access to resources, and oversight. Also to learn how legislation needs to change to take full advantage of this technology. Lastly, to assess the potential/feasibility cryptocurrency has to address the under banked. Improve Local Level Community Engagement, Access to resources, and oversight. Also to learn how legislation needs to change to take full advantage of this technology. Lastly, to assess the potential/ feasibility cryptocurrency has to address the under banked." This article employs that observation in terms of reviewing and posing reform of policy as related to blockchain information sharing processes and systems.

29 Fast and Waugaman, p. 119.

30 "FACT SHEET: U.S. Response to the Ebola Epidemic in West Africa.

31 This article does not discuss the technical assistance the U.S. provides for partners. Therefore, the authors delimited consideration of sharing collection and analysis technologies.

32 John J. Sullivan, remarks at the Blockchain Forum, 2017, The George C. Marshall Center, Washington, D.C., < https://www.state.gov/s/d/17/274725.htm>, accessed on June 3, 2018.