The Mitchell Forum

The Coming 5G Evolution in Network Centric Warfare: The Sensor Saturation Theory

By Lt Col Anthony Tingle, USA retired

About the Forum

The Forum presents innovative concepts and thought-provoking insight from aerospace experts here in the United States and across the globe. As a means to afford publishing opportunities for thoughtful perspectives, Mitchell Institute's Forum provides high visibility to writing efforts spanning issues from technology and operational concepts to defense policy and strategy.

The views expressed in this series are those of the authors alone, and do not necessarily represent the views of the Mitchell Institute for Aerospace Studies.

Abstract

The technological advances of 5G networking necessitate relooking at current philosophies on battlespace data gathering. Thousands of miniature interconnected sensors could provide new fidelity on the battlespace. This sensor saturation could provide a counterintuitive solution to the growing problem of wasted intelligence data collection. Through saturation the network is strengthened, although each individual sensor is devalued, and the metadata becomes more valuable than the actual data. With emerging technologies, analysts can approach data holistically, reducing their reliance on alerts to enemy activities and positions in the operating environment. This paper explains how new 5G technology will transform intelligence collection and provides a new perspective on battlespace data.

F-35As at Hill AFB, Utah, where they are developing 5G dynamic spectrum sharing capabilities between airborne radar systems and 5G cellular systems in the 3,100-3,450 MHz band.

U.S. Air Force Photo

Introduction

The U.S. government now has the ability to deliver munitions so precisely that it is using explosive-free Hellfire missiles with sharp blades to kill a specific passenger inside a vehicle without causing collateral damage.[1] As the physical means to destroy our enemies becomes ever more automatic, the identification, tracking, and targeting of these malcontents become the critical components of the kill chain. The quest for battlespace omniscience is not new; warriors have been attempting to "know the enemy" long before Sun Tzu ever immortalized the idea in the Art of War.

Prompted by the digital revolution and corresponding advances in data transfer, manipulation, and storage, information took a new form, and a new imperative, in the realm of warfare. The term Network Centric Warfare (NCW) began to circulate in earnest in the late 1990s as the U.S. military sought the same synergies found in commercial digital information sharing.[2] NCW became the cornerstone of military information infrastructure development.

Since its inception, the adoption and application of NCW throughout the U.S. military has been both rewarding and challenging. The services have embraced and adopted the concept unevenly. The Air Force adopted it early with successes in multiple conflicts including Operation Allied Force and Operation Iraqi Freedom.[3] Although the Army continues to struggle with the complexities of developing an information strategy for land forces, the military continues to evolve its information prowess.[4]

Today the more encompassing concept of information warfare dominates the discussion on military operations and technology acquisitions. As during the early days of NCW, technological developments in the civilian sector signal military advantages in information warfare. Recent commercial advances in networking and data analysis have spurred the U.S. military to consider how these technologies will lead to future battlespace dominance.

Fifth generation (5G) networking technology stands to revolutionize battlespace sensing and the way militaries approach data. Rapid growth of networking technologies is driven by factors such as powerful and small microelectronics, automated data manipulation and artificial intelligence, and advanced wireless connectivity. 5G networking technologies such as these will converge to enable future capabilities and presents a new theory of information dominance based on these projections.

The Evolution of NCW

In looking at the application of technology to warfare, it is necessary to ask two questions. First, what has changed? Second, why is this change significant? The short answer to the first question is that the technology of network operations, including the handling of data on those networks, is approaching a critical moment in its evolution. Specifically, 5G networking and its corresponding sensors are here, and like the commercial networking revolution of the late 1990s, they will undoubtedly change the nature of the civilian communications industry. The answer to the second question on the significance 5G is, at its core, that these networking technologies hold the opportunity to change the way we conduct military intelligence and targeting.

5G networking, like many modern innovations, is a confluence of multiple technologies. It uses miniature cell "towers" that consume less energy, and it exploits the advantages of beam forming to send signals only where necessary. It makes novel use of the electromagnetic spectrum, particularly in high and low frequencies. 5G networks

will also handle extreme amounts of traffic using massive multiple-input multiple-output (massive MIMO) architecture. It will also use different communication protocols to allow machines and nodes to easily connect to each other and eventually the "combat cloud."[5] The network will have lower power-requirements, lower latency (essentially the time to send information), and larger bandwidth.

These projections of 5G networking foretell future military capabilities and applications. For example, advances in reducing the size of radio components, such as in radio-frequency microelectromechanical systems, should allow for much smaller and more numerous sensors on the battlespace.[6] In the future, each person, vehicle, drone, or robotic entity on the battlespace would effectively have sensors and communication equipment, and they would be connected to all the other sensors.[7] Additionally, the reduced size and cost of 5G sensors could increase in the number of simple sensors across the battlespace. These small, low-power sensors could be delivered through airborne means into a conflict zone.[8] Each of these nodes will be connected to each other and simultaneously send data to the combat cloud.[9]

The future of the networked battlespace is a combination of thousands of sensors. These communication technologies will allow networks with endless nodes, each sending data to multiple vectors, effectively blanketing an area of operations with data gathering on a scale familiar to internet-based firms like Google, Facebook, or Amazon that depend on immense amounts of information. Similar to the information revolution of the 1990s, 5G military technology must follow close on the heels of commercial advancements.

Two Applicable Theories

Before delving into the possible military uses of 5G networking, it is useful to review two theories that have influenced network development. These theories primarily attempt to explain information transfer and the value of these networks. It is this previous theoretical work that underpins future theories that will guide the development of the next evolution of NCW.

Claude Shannon's Mathematical Theory of Communication

At the dawn of digital communication, MIT's Claude Shannon developed the most influential theory regarding the amount of information that can be transferred electronically. His theory starts by describing information in terms of discrete binary digits, also known as bits, in the form of 1s and 0s. He then expressed the number of bits (the signal) that could flow between destinations as the size of the river, or bandwidth. Finally, he theorized that this process could be muddied by outside factors, or noise.[10] In other words, interference reduces the transfer of information across a signal, and the higher the ratio of signal strength to interference, the more data that can be transferred. It will be important to refer back to Shannon's theory when discussing the amount of information that future networks provide, as this paper will later discuss the amount of noise that is actually created in current military systems by the signal itself.

Metcalfe's Law

In the earliest days of the internet, it became obvious that the rapid connectivity and information flow that digital communications provided could revolutionize military operations, as it was beginning to do with commerce. In an attempt to explain the value that networks

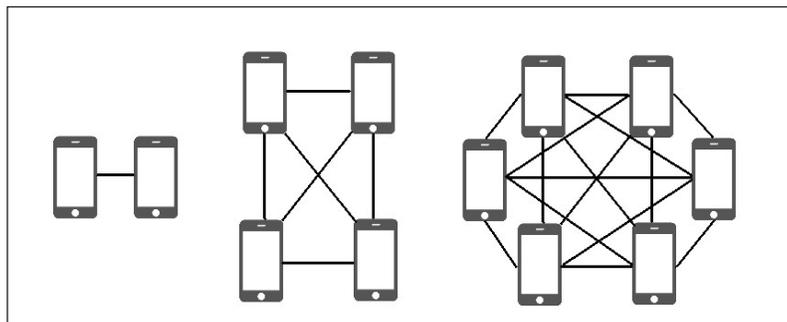provide, early NCW advocates relied on a rather simple theorem called Metcalfe's Law.[11]

Figure 1: Metcalf's Law. The value of the network increases exponentially with the number of additional nodes (N2).

Metcalfe's Law states that the value of a network increases exponentially with the increase in the number of interconnected nodes. The simplicity of the theorem allows for only limited network discussions, as many of the theorem's shortcomings are immediately obvious. First, the value of some nodes is inherently greater than others, especially nodes that provide greater information. For example, in a missile early warning network composed of land- and ship-based radar, the weaker ship-based radar may be of less value in terms of total detection capability. Additionally, the smaller the network, the more valuable the addition of another node is to the overall power of the network. In very large networks, like the type represented by the interconnected users on Facebook, it is difficult to believe that the addition of one more user represents an exponential increase in the value of the website. Additional theories have attempted to augment Metcalfe's, such as Zelf's Law, which states the value of each additional node in the network is less than the previous node.[12] But with all its shortcomings, Metcalfe's Law remains germane to network discussions due primarily to its simplicity (it is still used today to discuss large interconnected environments such as the Bitcoin phenomenon).[13]

Current Analysis of Battlespace Data

Between 1965 and 1972 the U.S. flew 871 unsuccessful sorties against the Thanh Hoa Bridge in Vietnam; only after the introduction later that year of laser-guided bombs was the bridge destroyed.[14] Other conflicts, such as the first Gulf War and Bosnia in the 1990s, showed that destroying the target is no longer the imperative to military success—finding the right target is what is paramount. Battlespace data is now the most important component in defeating an enemy, and the first step in developing a theory for the next evolution of military sensing is observing the way the military uses data in the battlespace. In its simplest form, data is used to locate, identify, and track the enemy.

An intuitive characteristic of intelligence is that, at each level of war, the fidelity of intelligence becomes more acute. For example, at the strategic level, large number of troop movements at a border would be significant, whereas the location and timing of individual vehicles along the border would simply confound the analysis. At the same time, at the tactical level of war, the location and vector of individual vehicles is of paramount importance. Throughout the levels of war, intelligence analysis purposefully gravitates toward aggregation. At each progressively higher level (e.g., from squadron to wing to numbered air force to joint air operations centers) analysts attempt to parse lower-level reports to get a consolidated picture of the operating environment.

In reviewing the uses of data in the battlespace, it is also useful to note the inherently predictive nature of intelligence. Intelligence analysts not only describe the battlespace, but attempt to predict enemy capability, intent, and future actions. In many ways, these functions are similar to the scientific method in terms of producing

conclusions or causality. Social scientists have rightly pointed out that making such assessments and reaching such conclusions "cannot be reduced either to strictly logical inference (deduction) or to empirical generalization (induction). Scientific inference is not only about applying formal logic; it also involves reasoning, creativity, the ability to abstract, and theoretical language in order to see meanings and structures in the seemingly unambiguous and flat empirical reality."[15] The point here is that data from the battlespace is used to make statements about reality. These statements are essentially an inference from a perceived or real sample of the population of interest, the battlespace.

Currently, making battlespace inferences is complicated by a flood of data. With the explosion of available sensor technologies, analysts are faced with an inability to use all the data they collect.[16] In this way, the signal begins to become the noise—a view shared and espoused by "the father of information theory" Claude Shannon, who first introduced theories of using raw data to represent actual information at MIT's Lincoln Laboratory. The more dire problem is that analysts are forced to try to decide which sensors provide them data that is the most valuable, and what information is most useful. They decide which supporting data is necessary to make predictions. In effect, they are predicting what supporting data they need to make predictions. In this way, battlespace intelligence becomes a system of probabilities in series and makes for an ever-destabilized intelligence cycle.

Here is where the future of battlespace networking gets interesting. The solution to this deluge of data may not be better, more powerful sensors, nor the ability select the most appropriate and accurate sensors at a given time and place. The solution to too many sensors may be more sensors.

The Sensor Saturation Theory of Battlespace Data

The underlying assumption necessary for a new theory of battlespace data collection is that existing or near-future technologies will revolutionize battlespace sensing. Specifically, these transformational technologies include the aforementioned 5G networking that, when you apply Moore's Law, enables the continued decline of cost and size of advanced electronic sensors and communication equipment, general advances in data processing and storage, and the realization of advanced data analytics, including artificial intelligence and machine-learning. The confluence of these technologies should allow for a massive network of small and inexpensive low-power sensors with a range of collection abilities including electro-optical, sonic, and thermal. These sensors could be emplaced or air-dropped by the thousands into an operation and could supplement the ever-expanding list of networked sensor sources including collection platforms, drones, and humans.

By effectively saturating the operational environment with sensors, we can produce a blanket of data collection. Because this data collection will approach a more complete picture of the conflict zone, analysts and operators will no longer search for the enemy as much as remove benign data. In other words, instead of searching for the glint of the needle in the haystack, analysts will simply remove the hay. In effect, battlespace collection becomes the inverse of present-day collection methods that look for abnormalities to reveal themselves, relying more on analysis and correlations to a "baseline" of the battlespace.

Impact on Prediction

The application of this theory has two major ramifications. First, rather obviously, is that this sensor saturation will both

reduce the necessity for and increase the accuracy of battlespace predication. It stands to reason that with greater knowledge of the battlespace, the location and description of nefarious actors will be easier to discern. Additionally, any knowledge gaps will be more readily filled with bolstered predictions. This new network will increase our certainty of known enemies and help predict enemy actions.

In discussing the validity of the predictive value of more sensors, it is useful to compare battlespace prediction with an equally valued arena of prediction such as the stock market. In financial markets, both data and analysts are legion. In the models used for the stock market, the goal is to predict price movements of stocks or indices. In this regard, the objective function for stock prediction (the future stock price) is explicitly well-defined. Knowledge is power and more information is usually better, but large amounts of data have not allowed anyone to predict stock price movements with any regularity. Stock picking remains a "random walk." Why?

First, the inputs (or sensors) of stock picking are not all-inclusively telling of the objective function. In other words, the sensor inputs do not directly predict price movements. The specific inputs also do not account for the additional inputs of market fluctuation. Let's take the price of corn futures, for example. Sensor inputs to the price of corn futures could include imagery on the condition of local and global corn fields, as well as applicable weather predictions. Given the basic principle of supply and demand, if total knowledge was known about the future global corn-crop yield, and the total future demand for corn, analysts could still not completely determine the future price. Perhaps the most influential reason for this predictive shortcoming is what John Maynard Keynes called "animal

spirits," or the human emotional factor in the trading of stock prices.[17] Additionally, other unavailable information contributes to stock price movements: unpredictable industry expansions, regulatory decisions, and natural disasters, for example. Generally, however, the greater amount of specific information influencing a stock sector (e.g., corn crop yield), the greater probability of success.

Now, let us compare the military data problem to that of stock price fluctuation. In the absence of more complex political-military issues, the central objective function of military data collection is to identify and locate specific entities across the battlespace—a very specific objective with a well-defined end state, similar to stock picking. Yet, unlike the large number of stock information inputs, the sensor inputs more directly contribute to the objective. These sensors discover the identity and location of the target at a specific time. In the absence of battlespace deception, detection and identification of a target are the primary considerations in the objective of the data collection.

The bottom line of this reasoning is that if financial analysts have been unable to predict stock prices given the amount of information, analysis, and raw resources available, then how will militaries be able to predict enemy actions, movements, or intents? Given enough sensors and the proper "infostructure," battlespace intelligence will transform from a system that detects sensor inputs to one that detects environmental abnormalities, develops useful correlations in the data, and provides a holistic analysis of the operating environment.

The Value of Individual Sensors in the Network

The U.S. military seemingly has a surplus of battlespace data such that the inclusion of more data may mean more distraction, creating more of a detriment

to the intelligence community. In Claude Shannon terms of communication theory, the amount of information transferred is reduced by an increase in the data and a corresponding increase in the noise of the system. As Henrik Jeldtoft Jensen, a professor of mathematical physics states:

> Understanding the behaviour of a complex system necessitates a simultaneous understanding of the environment of the system. In model studies, one assumes often that the surroundings can be represented by one or the other type of "noise," but this is just a trick that allows one to proceed with the analysis without understanding the full system under consideration. It is very important to appreciate that the "drive" or the "noise" are equally crucial to the understanding, as is the analysis of the "system" itself.[18]

So if the system itself begins to become the noise, then the information in the system is reduced, and so is the value of the network.

At this point, it is necessary to focus on the addendum to Metcalfe's Law called Zelf's Law, also known as the "long tail" theory of the value of the lower-tiered contributors to the network. Zelf's Law posits that each additional node on a network decreases in relative value.[19] In terms of the battlespace sensor mosaic, an analogy for Zelf's Law is the television pixel. In the extreme case of a one-pixel network, that one pixel would be extremely valuable, perhaps indicating on or off, day or night. As we add pixels to this imaginary battlespace TV, each additional pixel helps describe and form the picture. The value of

the entire system increases exponentially, as predicted by Metcalfe. Yet, as we reach the fidelity of modern televisions with effectively thousands of pixels, the value of each individual pixel is reduced. In terms of discerning the actual picture, the value of one of these pixels effectively goes to zero—one pixel barely contributes to the overall picture.

Likewise, in extremely large battlespace data collection networks, the value of the average individual sensor approaches zero. In these types of networks, the "message internals," or the actual data that the average sensor is transmitting, is of ever-decreasing value. Conversely, the "message externals," or those parts of the message that describe the message itself such as date, time, and location of sensor, become more important. The network becomes Boolean, with each sensor simply on or off (detecting or idle).

What this sensor saturation theory describes for future battlespace sensing is a television picture with thousands of pixels (sensors). Each of these sensors is simply on or off—transmitting message externals—at a given time. It is the activation pattern of these sensors that allow for detection—by removing the hay to find the needle—or predictive analysis. The predictive analysis on these thousands of data points is similar to the big data analysis that Amazon.com does on its customers. By discerning patterns and correlations in their data, Amazon can predict when and what type of product their customers will need, often before the customer knows what they need.[20]

In figure 2, the power and the value of each node closely follows Metcalfe's law during the early growth of the network. As the network becomes more saturated with sensors, the value of each sensor begins to decrease. The power also stagnates due

Figure 2. The contribution of individual sensors to the overall intelligence collection network.
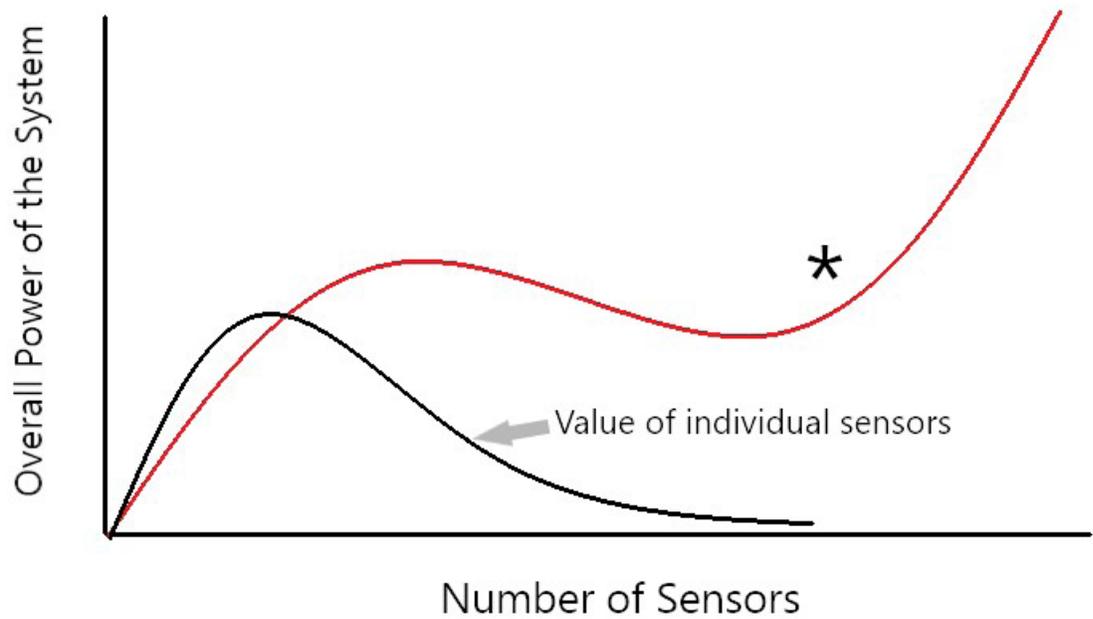
to the burden on the overall intelligence collection network created by the ever-greater number of sensors. Then, at the inflection point—marked by the asterisk—we see another exponential leap in the power of the network as sensor count reaches full saturation. This is the theoretical point where there are so many sensors covering such a density of the battlespace that the analysis precludes sensor internals in favor of sensor externals. Concurrently, at a certain point, the value of each individual sensor approaches zero.

Discussion

5G networking technology could enable a torrent of new battlespace capabilities. First, 5G inherently produces more coordinated and succinct data. Something very interesting happens when theorizing a message externals-only network. One of the fundamental data fusion problems, configuring the data to be compatible across a network, becomes less formidable as 5G networking uses a standardized protocol (IP).[21] Additionally, the data that comprise the message externals are minute compared to the internals. Thus, this future network may have the added

bonus of less overall actual bits transmitted per sensor. The military will no longer rely on complex data from individual sensors, rather the large sensor network completes the picture of the battlespace like the many pixels of a television.

Second, artificial intelligence should be able to refine network results and contribute to overall intelligence gathering. Artificial intelligence (AI) can better optimize the extremely large networks of the future by manipulating connections to an otherwise unmanageable number of sensor inputs and maximize efficiency and collection. Although less important in future networks because message externals are extremely simple, AI can also smooth data melding by recognizing different forms of data and converting them to useful information. Lastly, it will be able to make predictions based on big data analysis of the network data.

As previously mentioned, aggregated battlespace intelligence is composed of data from lower echelons, with the finest data comprising the "bit" of intelligence. Until now, militaries have lacked complete fidelity across the battlespace, relying instead on consolidating spikes of intelligence. Analysts evaluate each data source relative to other

sources of information. Militaries have failed to approach intelligence collection in terms of the absolute aggregate: in other words, having near-complete intelligence. Having a more detailed picture of the battlespace will require intelligence entities to change their perspective from seeking items of interest (e.g., persons of interest, enemy vehicles, nefarious patterns of life) to monitoring the entire environment and effectively removing the impertinent data. In other words, instead of looking for the enemy needle in a haystack, we are removing the hay, leaving only the bad actors. This is essentially the inverse of the way we approach intelligence today.

Lastly, and most obviously, militaries must develop new combat networks that emphasize mobility. 5G cell towers are much smaller than previous generations and should allow for vehicles, robots, and humans in the battlespace to carry small, mobile repeater stations.[22] Militaries will need to develop capabilities and tactics, techniques, and procedures to mitigate the inability of millimeter wave frequencies to penetrate walls and other structures. The development of combat employment of 5G capabilities should be ongoing and open to new insights as more and more capabilities are fielded and saturation becomes ubiquitous.

Conclusion

Up to this point it has been unnecessary, and possibly ridiculous, to speak in terms of data collection and analysis in terms of a complete mosaic of data covering the entire battlespace. The current and future technological advances of 5G networking may necessitate re-looking current philosophies on battlespace intelligence. Thousands of miniature interconnected sensors could provide new fidelity on the targeting cycle. Additionally, this large network may provide a counterintuitive solution to the growing problem of wasted intelligence data collection. By flooding the battlespace with sensors, the network is strengthened although each individual sensor is devalued; the message externals become more valuable than the internals. With these emerging technologies, analysts will approach data holistically, reducing the need for analysts to rely on intelligence spikes in the operating environment.

Moving ahead, the problem is twofold. First, the military will very likely lag behind the commercial sector in developing sufficient "infostructure" to take advantage of massive sensor data, including shortfalls in data storage and AI computational power. Second, military organizations lack necessary and sufficient theories on large data, AI learning, and prediction models. The military and intelligence communities can begin remedying the later problem today by accelerating testing and acceptance of universal models. Doing so will ultimately allow proper and efficient expenditure of the national defense budget.

Much like in civilian markets, the earlier the U.S. military prepares for and acts on this networking eventuality, the greater its future advantages over its rivals. Success will require a holistic approach focused not only on acquisitions and research and development, but also systemic changes, including those in doctrine, organization, and tactics. An underlying theory of data collection and analysis that accounts for future technologies will guide the development of the next evolution in NCW. ✪

Endnotes

1   Gordon Lubold and Warren P. Strobel, "Secret U.S. Missile Aims to Kill Only Terrorists, Not Nearby Civilians," *The Wall Street Journal*, May 9, 2019.

2   David S. Alberts, John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd edition (Washington, DC: DOD, C4ISR Cooperative Research Program, February 2000).

3   Clay Wilson, *Network Centric Operations: Background and Oversight Issues for Congress* (Washington, DC: Congressional Research Service, 2007).

4   Loren Thompson, "5 Reasons the Army's New Battlefield Networking Strategy Won't Work," *Forbes*, November 20, 2017.

5   Vincent W.S. Wong, Robert Schober, Derrick Wing Kwan Ng, and Li-Chun Wang, eds., *Key Technologies for 5G Wireless Systems* (Cambridge, UK: Cambridge University Press, 2017); and David A. Deptula, *Evolving Technologies and Warfare in the 21st Century: Introducing the "Combat Cloud"* (Arlington, VA: Mitchell Institute, 2016).

6   Stoyan Nihtianov and Antonio Luque, *Smart Sensors and MEMS: Intelligent Sensing Devices and Microsystems for Industrial Applications* (Cambridge, UK: Woodhead Publishing, 2018).

7   Amélia Ramos, Tiago Varum, and João Matos, "Compact Multilayer Yagi-Uda Based Antenna for IoT/5G Sensors," *Sensors* 18, no. 9, 2018.

8   Yoshiaki Taniguchi, Tomoya Kitani, and Kenji Leibnitz, "A Uniform Airdrop Deployment Method for Large-Scale Wireless Sensor Networks," *International Journal of Sensor Networks* 9, no. 3–4, 2011.

9   Ali Kashif Bashir et al., "An Optimal Multitier Resource Allocation of Cloud RAN in 5G Using Machine Learning," *Transactions on Emerging Telecommunications Technologies*, May 2019.

10 Claude Elwood Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal* 27, no. 3, 1948.

11 Alberts, Garstka, and Stein, Network Centric Warfare.

12 Bob Briscoe, Andrew Odlyzko, and Benjamin Tilly, "Metcalfe's Law Is Wrong," *IEEE Spectrum*, July 1, 2006.

13 Spencer Wheatley et al., "Are Bitcoin Bubbles Predictable? Combining a Generalized Metcalfe's Law and the LPPLS Model," *SSRN Electronic Journal*, March 2018.

14 David A. Deptula and Douglas A. Birkey, *Resolving America's Defense Strategy-Resource Mismatch: The Case for Cost-Per-Effect Analysis* (Arlington, VA: Mitchell Institute, 2020).

15 Berth Danermark, Mats Ekstrom, and Liselotte Jakobsen, *Explaining Society: An Introduction to Critical Realism in the Social Sciences* (New York: Routledge, 2005), 113.

16 Isaac Porche et al., *Data Flood: Helping the Navy Address the Rising Tide of Sensor Information* (Santa Monica, CA: Rand Corporation, 2014).

17 John Maynard Keynes, *The General Theory of Employment, Interest, and Money* (San Diego, CA: Houghton Mifflin Harcourt, 1964).

18 James Moffat, *Complexity Theory and Network Centric Warfare* (Darby, PA: DIANE Publishing, 2010), xiii.

19 Briscoe, Odlyzko, and Tilly, "Metcalfe's Law Is Wrong."

20 Thomas H. Davenport, "Competing on Analytics," *Harvard Business Review* 84, no. 1, 2006.

21 Martin Liggins II, David Hall, and James Llinas, *Handbook of Multisensor Data Fusion: Theory and Practice*, Second Edition (Boca Raton, FL: CRC Press, 2017).

22 Allan Holmes, "5G Cell Service Is Coming. Who Decides Where It Goes?" T*he New York Times*, March 2, 2018.

About the Author

Anthony Tingle is a retired U.S. Army Lieutenant Colonel, formerly the Concepts Evaluation Branch Chief at U.S. Army Space and Missile Defense Command. He holds a PhD in public policy form George Mason University, an M.Eng and an MBA from the University of Colorado, Colorado Springs, and a B.S. in systems engineering from West Point. He writes on research, development, and the application of technology within the Department of Defense. The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.