Intelligence After Next

SERIES
23

DECIPHERING UBIQUITOUS TECHNICAL SURVEILLANCE (UTS) WITH DATA-DRIVEN ANALYTICS AND ARTIFICIAL INTELLIGENCE (D2A2)

by Shawn Benson

 # 24-1387 4-10-2024

Detectable versus Deducible Intelligence

To understand the threat posed by our adversaries' global technical surveillance capabilities, Department of Defense (DoD) and Intelligence Community (IC) leaders must seek to understand and differentiate their Data-driven Analysis and Artificial Intelligence (D2A2) capabilities. D2A2 is the proverbial "beating heart" of our rivals' growing ability to leverage data produced by the internet of things (IoT) and state-level technical surveillance (e.g., CCTV, lawful intercept of civilian communications, otherwise known as ubiquitous technical surveillance (UTS).[1,2] Without D2A2, the data produced by UTS would be nearly unintelligible and unactionable. In other words, our leaders in the DoD and IC must not only devote resources to determining what is detectable (by UTS) but also rapidly advance our understanding of what is deducible (by D2A2).

This new term, D2A2, for an already established concept, provides the DoD and IC a framework for ascertaining what is deducible and allows demarcation of the resulting analysis. What we stand to learn from that analysis will be powerful: mapping our adversaries' D2A2 capabilities will reveal exploitable gaps in their data processing capabilities. In sum, D2A2 gives the DoD and IC a true path forward, rather than defaulting to the erroneous, fatalistic, and defeatist presumption that anything detected by a UTS sensor is consequently compromised.

Adversarial Threats through Advances in Technology

For decades, it was fashionable among national security professionals to remark that "the Cold War is over" when critiquing an out-of-date methodology or process inside the DoD or IC. As former Director of the Central Intelligence Agency James Woolsey once famously said about the realignment of mission after our victory over the Union of Soviet Socialist Republics (USSR), "We have slain a large dragon. But we live now in a jungle filled with a bewildering variety of poisonous snakes. And in many ways, the dragon was easier to keep track of."[3] Woolsey was unquestionably right. Today, we stand on the precipice of a similar inflection point: we have spent decades tracking down Woolsey's poisonous snakes, only to find the formerly slain dragon has resurrected (Russia) and multiplied (China). Today, we face an array of "near peer" adversaries that can hold at risk not only the products of our national security apparatus but also the processes by which we produce and deliver them. Not since World War II has the United States been as broadly vulnerable to our major adversaries through advances in technology, like UTS.

We must avoid the assumption that simply because our adversaries can "see" us, those same adversaries can also "understand" what they are seeing. We cannot afford to presume that detection equals deduction. We cannot assume observation equals compromise. We must understand not only what the adversary can perceive, but what they can comprehend.

In this new world of pervasive surveillance, it was not a series of repressive dictators who installed UTS, but rather free citizens who peacefully surrendered their privacy and data for the promise of an easier, faster, and sensor-rich lifestyle. But even as world leaders and citizens alike are increasingly questioning the prudence of living in such a world, national security concerns and commercial interests will predictably drive more sensors into every facet of our lives. UTS is here to stay.

In response to this threat, DoD and IC scientists, technologists, and analysts focus time and resources on ways to avoid sensors, obfuscate digital signatures,

and otherwise "fool" UTS. It is questionable whether this technological arms race is viable in the short term, even if it is both necessary and understandable. However, in the medium-to-long term, such a competition is almost certainly fraught. It is likely that vested financial interests and nation-states will drive data-processing and artificial intelligence (AI) advances, which will obliviate defensive advances against many sensors or their AI-driven processes. We are likely to live in a world of increasingly inescapable surveillance, as offensive advances most often outpace defensive efforts.

In such a future, international competition and conflicts will certainly not disappear, even as our ability to spy on one another accelerates and differentiates. In this not-so-distant future, we will still require the DoD and IC to successfully conduct their missions. It will be even more critical that we follow the advice of military strategists and "fight [the] enemy where they are not" and "understand our enemy and ourselves" if we are to find and exploit gaps in our adversaries' armor.[4]

As the net of UTS closes, through the inescapable and voluntary adoption of technologies embedded with increasingly sophisticated sensors, we must turn our attention to our adversaries' (and our own) ability to process the data that UTS generates. We must avoid the defeatism that drives the assumption that simply because our adversary can "see" DoD and IC personnel planning, resourcing, and conducting their missions, those same adversaries can also "understand" what they are seeing. We cannot afford to presume that detection equals deduction. We cannot assume observation equals compromise. We must understand not only what the adversary can perceive but what they can comprehend. To understand the difference between what UTS collects and the intelligence the resulting data generates, we must understand how UTS data becomes intelligence. We must understand the vast complexities and uneven global landscape of D2A2.

TCPED, UTS, and D2A2

The DoD and the many intelligence agencies supporting its critical work use the term Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED) to conceptualize their phased approach to intelligence work.[5] This framework allows intelligence professionals to align personnel and materiel to specific phases of the "intelligence cycle" to advance the mission of collecting, analyzing, and distributing timely, actionable information to decision makers. Breaking the intelligence cycle down into discrete phases also allows intelligence professionals to see linkages and dependencies, and to identify challenges or places for improvement within the cycle. By arranging UTS and D2A2 as linear, linked processes, U.S. intelligence professionals can overlay UTS and D2A2 over the TCPED framework to accrue many benefits.

UTS defines the pervasive sensor network, which consists of an array of devices. These devices range from those traditionally associated with intelligence work (e.g., CCTVs, satellites, lawful telephone intercept capabilities, other signals intelligence capabilities) to those individual people carry with them every day (e.g., smart phones, smart watches, in-home digital assistants, smart TVs, in-vehicle entertainment/smart phone integration suites). Rather than a unified network, UTS describes an environment where both the IoT and state-level surveillance merge to create a world of nearly inescapable data collection. However, UTS does not adequately describe what individuals, groups, businesses, or states can do with the data. The assumption is that UTS data is exploited, but to adequately understand the gaps in this intelligence collection system, we must move beyond the concept of collection. We cannot stop at the "TC" of TCPED; we need to understand the "PED" of the intelligence cycle. We need D2A2.

D2A2 describes processes and systems of data analytics, augmented (or not) by AI. Within the field of data science and data analytics are nested concepts and processes. Within the field of AI, there are numerous

subfields dealing with specific types of machine intelligence. Those range from aspirational general intelligence and large language models to more simplistic machine learning algorithms. As a result, the term Data-driven Analytics and AI merges two established fields that, today, are increasingly inseparable. Once merged, we can use D2A2 to capture what happens to data produced by UTS as it is processed, exploited for insights, and ultimately distributed (a process likely be augmented by AI in the future). This term not only adequately captures the "PED" portion of the UTS/D2A2 TCPED cycle, but it future-proofs the terminology to some degree, as both data and AI will be driving threats to DoD and IC missions for the foreseeable future. In other words, while data-driven analytics are presently a problem for the U.S. national security community, it is not difficult to foresee a future where AI augments those data-driven efforts to a sufficient extent that understanding the "PED" of UTS data is inextricably tied to AI.

Perhaps most importantly, distinguishing D2A2 from UTS will allow us to conceptualize adversarial capabilities along the spectrum of data analytics/data science processes, with or without augmentation by AI. Such a conceptualization will allow us to ask ourselves questions like:

- What are a given adversary's resources in the realm of D2A2?
- What sensors does an adversary trust most for their offensive and defense counterintelligence work? (And, by extension, which specific sensors should we try to defeat or fool?)
- Does an adversary possess the appropriate and continued funding, talent pipeline, access to hardware, access to data, and regulatory framework (or lack of it) that allows data collected by UTS to be turned into actionable intelligence?
- If an adversary can create actionable intelligence from UTS data, what is that adversary's ability to do so in real time versus the performance of forensic reconstruction?
- Does the adversary in-question have integrated systems capable of both producing and disseminating such information to parts of their organization or state security apparatus to do anything about the intelligence they have gleaned?

Conversely, we can use such a framework to analyze ourselves—and rapidly close gaps in our own capabilities. By delineating what falls into the category of D2A2 versus what falls into UTS, we can divide these realms of knowledge for maximum effect, while maintaining connectivity between the disciplines.

Without understanding how UTS data becomes intelligence (i.e., via D2A2), we assume anything UTS detects is, therefore, compromised. In reality, substantial holes exist in our adversaries' D2A2 capabilities, creating gaps for the DoD and IC to exploit both offensively and defensively.

Concepts and Cognition: An Argument for Differentiation

As far back as ancient Greece, thinkers like Aristotle knew the importance of finding "differentia," or the characteristics that allow for the proper division of concepts. In ancient Greece, it was considered a logical mistake to lump together too much, just as it was an error to define something too narrowly.[6] So, when the DoD and IC first encountered the threat of pervasive surveillance and its effects, they brought themselves credit by capturing the concept as "ubiquitous technical surveillance." Naming the concept allowed the DoD and

IC to devote resources to the issue and build sizable knowledge, and it was an accurate description of the problem. However, between those early days and now, at least two significant developments have occurred: 1) the technologies underpinning UTS have evolved, which has diversified both the threat and opportunity landscape; and 2) knowledge of UTS has grown substantially. As a result of these changes, UTS is ready to undergo another evolution and traverse a gate through which many fields of knowledge pass: differentiation.

Like the fields of mathematics, engineering, and computer science, UTS must undergo a re-evaluation and subsequent subdivision so that it can mature. These divisions should start with D2A2. D2A2 allows members of the DoD and IC to separate from UTS the "surveillance" that UTS accomplishes from the result of that surveillance: actionable intelligence. This division is logical as surveillance/reconnaissance (aka "collection") and analysis of surveillance/reconnaissance data (aka "processing" or "exploitation") are already distinct concepts inside the DoD and IC. Second, pulling D2A2 away from UTS allows the overall field to benefit. Technical and engineering professionals can specialize and deepen their knowledge of UTS, while data-centric analytical professionals can explore the equally vast complexities of D2A2. But, by keeping these terms associated, we can still allow advances in UTS to complement D2A2 and vice versa.

Another reason for differentiation is rooted in its cognitive benefits. While proper conceptualization has many institutional and resource allocation benefits, there are profound cognitive benefits associated with meaningful differentiation, and cognitive challenges associated with improperly terming concepts. At a high level, those benefits are related to the way language and cognitive processes affect one another.[7] Human beings have limited cognitive resources, particularly in working memory,[8] so "overstuffed terms" become particularly problematic. Put simply, humans are categorizing machines,[9] and when terms are not well defined (or become ill defined), working with those terms becomes far more complicated. However, when we categorize concepts correctly, we can make predictions about things inside categories and shared communication flows appropriately.[10]

The combination of these epistemological and psychological benefits underscores one final motivator for differentiation of D2A2 from UTS: the Data, Information, Knowledge, Wisdom (DIKW) pyramid. The linear DIKW process explains how data can be processed to create information, which, in turn, is turned into knowledge and, finally, wisdom—the ultimate goal of data collection.[11] The simplistic process of DIKW explains why, in the absence of D2A2, the DoD and IC have struggled with UTS: without understanding how UTS data becomes wisdom (aka "intelligence"), we assume that it becomes intelligence. This assumption makes UTS unmanageable in a world where avoiding being observed by UTS is nearly impossible. Put another way, without understanding how UTS data becomes intelligence (i.e., via D2A2), we assume anything UTS detects is, therefore, compromised. In reality, substantial holes exist in our adversaries' D2A2 capabilities, creating gaps for the DoD and IC to exploit both offensively and defensively.

We Must Separate D2A2 from UTS

The DoD and IC are grappling with UTS, its threats, and its opportunities. The effects of UTS are numerous and varied, and they unfold rapidly. Many members of the DoD and IC continually struggle to come to grips with the enormity of the concept, often expressing frustration at not knowing "where do we even start" to address a problem that seems limitless. At first, this seemingly overwhelming challenge was due to UTS's novelty. Today, the increasing complexity of pervasive technical surveillance and the state-of-the-art analytical efforts that underpin its effectiveness defy simple explanation and easy comprehension.

Compounding the problems presented by an undifferentiated UTS ecosystem, it is likely that the size of the UTS problem set has contributed to a sense of futility or helplessness inside the DoD and IC. Undifferentiation may have also made it difficult for the DoD and IC to identify ways that adversarial UTS/D2A2 infrastructure itself is vulnerable. Additionally, not only does an undifferentiated discipline stymie the building of institutional knowledge and contribute to miscommunications, but it also tends to be cognitively detrimental—a problem without firm boundaries tends to appear unlimited and, therefore, insurmountable. At bottom, we see that when professional terms become "overstuffed," they also become inaccurate and unwieldy, rendering them unhelpful.

UTS is no longer an adequate term to define the entirety of the "UTS problem." To address this inadequacy, we must evolve our understanding of UTS and embrace "professionalization" of the UTS field. To accomplish this evolution, a good first step is to recognize that data generated by UTS does not, without significant effort, become actionable insight for our adversaries. Creating value from UTS data requires specific talents, skills, materials, technology, budgets, access to data, and an ability to distribute the resulting information to a receptive audience. Put another way, UTS requires a subsequent process, D2A2, to create meaningful and actionable intelligence. If the DoD and IC embrace differentiation of UTS and recognize D2A2 as a separate, but linked, concept, the U.S. national security community will find itself positioned to overcome previously insurmountable obstacles, plan DoD and IC missions effectively, and showcase U.S. adaptability and leadership in tackling pernicious challenges posed by technological threats.

References

1. Warren P. Strobel, Biometrics, Smartphones, Surveillance Cameras Pose New Obstacles for U.S. Spies, November 27, 2021. Available: https://www.wsj.com/articles/biometrics-smartphones-surveillance-cameras-pose-new-obstacles-for-u-s-spies-11638009002
2. William J. Burns, The Role of Intelligence at a Transformational Moment, April 14, 2022. Available: https://www.cia.gov/static/Director-Burns-Speech-and-QA-Georgia-Tech.pdf
3. Worley, K. (2020, September 2). Dueling with dragons and sparring with snakes: US strategy in an era of varied threats. Modern War Institute. https://mwi.westpoint.edu/dueling-with-dragons-and-sparring-with-snakes-us-strategy-in-an-era-of-varied-threats/
4. Sun Tzu, The Art of War, Fall River Press, 2015.
5. Daniel J. Henry, ISR Systems—Past, Present, and Future, Rockwell Collins Thought Leadership, 2017. Available: https://rockwellcollinsthoughtleadership.files.wordpress.com/2017/07/isr-systems-past-present-and-future.pdf
6. John E. Hare, Aristotle and the Definition of Natural Things, Phronesis, 24(2), 168–179, 1979. Available: http://www.jstor.org/stable/4182065
7. A. B. Markman and B. H. Ross, Category Use and Category Learning, Psychological Bulletin, 129(4), 592–613, 2003. Available: https://doi.org/10.1037/0033-2909.129.4.592
8. G. A. Miller, The Magical Number Seven Plus or Minus Two: Some Limits on Our Capacity for Processing Information, Psychological Review, 63(2), 81–97, 1956. Available: https://doi.org/10.1037/h0043158
9. Stevan Harnad, To Cognize Is to Categorize: Cognition Is Categorization, In C. Lefebvre & H. Cohen (Eds.), Handbook on Categorization, Elsevier, 2005.
10. A. B. Markman and B. H. Ross, Category Use and Category Learning, Psychological Bulletin, 129(4), 592–613, 2003. Available: https://doi.org/10.1037/0033-2909.129.4.592
11. Jonathan Hey, The Data, Information, Knowledge, Wisdom Chain: The Metaphorical Link, The DIKW Chain: The Metaphorical Link, December 2004. Available: https://www.jonohey.com/files/DIKW-chain-Hey-2004.pdf

Author

Shawn Benson is a principal systems engineer in Strategic Intelligence at MITRE. Shawn previously served in the U.S. Department of State as a Foreign Service Officer and, prior to that, in the U.S. Air Force as a Network Intelligence Analyst.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

JUNE 2024