

United States Military Academy

**USMA Digital Commons**

---

Army Cyber Institute

---

8-14-2023

## **6G Systems and the Future of Multidimensional Attack Planes**

Joshua Palochak

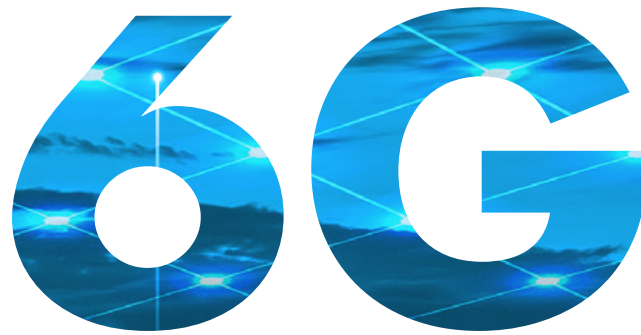
Jason Brown

Brian David Johnson

John Marx

Annette Aranda





# SYSTEMS AND THE FUTURE OF MULTIDIMENSIONAL ATTACK PLANES



Authors:

Joshua Palochak, Jason C. Brown, Brian David Johnson, John Marx, and Annette Aranda

# LIST OF PARTICIPANTS

**Albert Varma, Phaedrus, LLC**

**Alex Ruiz, Phaedrus, LLC**

**Alisha Bhagat: Parsons School of Design**

**Sergeant Major Amanda Draeger, Army Cyber Institute**

**Andrew Thiessen, The MITRE Corporation**

**Angelos Keomytis, GA Tech**

**Ann-Elisabeth Samson, McMaster University of Toronto**

**Annette Aranda, Phaedrus, LLC**

**Anonymous**

**Audrianna Kelly Matthew Mossholder, PJM**

**Brian David Johnson, Phaedrus, LLC**

**Dr. Bryson Payne, University of North Georgia**

**Christine Limsiaco, Lockheed Martin**

**Cyndi Coon, Laboratory 5**

**Damian L.**

**Denis P. Garman, Lockheed Martin**

**Drew Brown, CISA**

**Ethan Payne, Virginia Tech**

**Gary D. Markowitz**

**Hana S. Alverina, The MITRE Corporation**

**LTC Hugues Didio, NATO**

**Ian MacLeod, Packet Forensics**

**Jamil Brown**

**Dr. Jason C. Brown Lt. Col., Army Cyber Institute  
John Marx, Phaedrus, LLC**

**Joshua McKinley, Citadel**

**Dr. Joshua “Griz” Palochak, Phaedrus, LLC**

**Joshua Ryan, Norwich University**

**Julie Jenson, Concrete**

**Michael Silva, Texas A&M University**

**Michael Woudenberg**

**Michelle McCluer, Mastercard**

**Radha Mistry**

**Raul Jimenez, NATO**

**Richard Vorder Bruegge, FBI**

**Ron Smith, FBI**

**Ross Chamberlain, Phaedrus, LLC**

**Ryan Barrett Kennedy, Sandia National Laboratories**

**Simona Dean, Lockheed Martin**

**Thomas Motta, FBI**

**Vilma Luoma-Aho, Jyväskylä University School of Business and Economics**

## Disclaimers:

The views expressed herein are those of the analyst authors and do not reflect the position of NATO, the United States Military Academy, the Department of the Army, or any U.S. company, educational institution, or office of the United States Government.



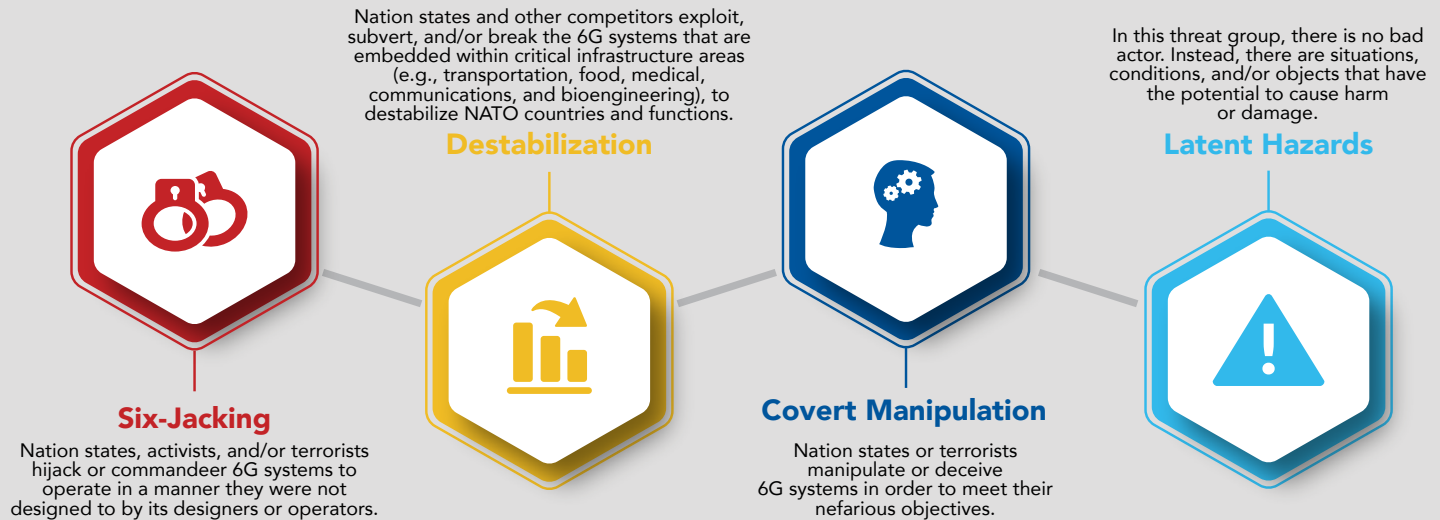
# TABLE OF CONTENTS

Executive Summary	1
Poem	3
Introduction	4
6G Overview	5
Introduction to the Threatcasting Method	6
What is the Threatcasting Foundation?	8
Functional Definitions	10
Prompts and SME Interviews	12
Findings	16
Discussion	20
Backcasting the Way Forward: Actions and Implications	27
Conclusion	36
Appendix A - SME Transcripts	37



# Executive Summary

In the coming decade, future threats from attacks on 6G communications systems appear in four categories or groups. The threats are specific to government, military, and critical infrastructure.



## **SIX-JACKING AS A NOVEL TACTIC DURING COMPETITION AND CONFLICT**

Adversaries of the U.S. and NATO (e.g., nation states, activists, non-nation state competitors, and/or terrorists)<sup>1</sup> hijack or commandeer 6G systems to operate in a manner they were not designed to and/or expected to by its designers or operators. In these cases, the 6G system is still functioning, but someone else has taken control of the system in whole or in part to point it in a different direction and/or use it for their advantage. Similar to hijacking a vessel in transit, six-jacking refers to this act within the 6G eco-system.

## **6G SYSTEMS ENABLE DESTABILIZATION**

Adversaries exploit, subvert, or break 6G systems embedded within critical infrastructure areas (e.g., transportation, food, medical, communications, and/or bioengineering), to destabilize NATO countries and functions. Destabilization manifests as geopolitical weakening, military dysfunction, reduced resilience across a country, disrupted supply chains, or general chaos.

## **6G SYSTEMS CREATE OPPORTUNITIES FOR COVERT MANIPULATION**

Adversaries manipulate or deceive 6G systems to bring about their nefarious objectives. These objectives are expected to be widespread in nature. Purposes range from achieving geopolitical gains, conducting intelligence gathering, and undermining trust in critical infrastructure to enabling terror acts, creating conditions for bad military decision making, lessening resilience, and weakening military effectiveness. To the operator, these influenced 6G systems appear to be functioning correctly and it is only later that they realize there is a problem. Therefore, the manipulation is performed within a layer that is not obvious or viewable by the operator, which in turn, creates increased vulnerability.

## **OVER-RELIANCE CREATES LATENT HAZARDS**

In this threat group, there is no bad actor. Instead, there are situations, conditions, or objects that have the potential to cause harm or damage. Latency

<sup>1</sup> These particular actors were called out in our participant raw data, but they are not all inclusive of the types of adversaries that NATO members will need to consider and contend with.

indicates that the hazard is hidden or dormant, but has the potential to become active or visible under certain conditions. First, government, military, and critical infrastructure supervisors have an over reliance on 6G systems, which creates one of the conditions that may cause other latent hazards to become active or visible.

Second, future problematic medical conditions due to electromagnetic exposure of 6G signals may induce unknown health hazards. Third, 6G systems will be highly desirable in their efficiency and effectiveness, and the speed, scope, and scale of their use is likely to desensitize friendly assets to their ubiquitous presence. This could create a situation that allows for a surprise attack surface that is not previously seen in military operations. Finally, an ubiquitous dependence on 6G systems may create a condition where the loss of access to these systems may affect the speed and accuracy of decision making.

It is recommended, therefore, that NATO, academics, and industry partners take the following actions in order to Out-Think, Out-Excel, Out-Fight, Out-Pace, Out-Partner, and Out-Last adversaries:

- Create a unified vision for 6G systems and their enablers. This vision should encompass access, employment, and implications for equitable use across NATO members and their societies.
- Go beyond DIME to understand the variety of factors that 6G systems will have on NATO strategies and activities, such as legal and law enforcement, scientific and technical, political, social, or environmental.
- Enable knowledge and information sharing that involves educating the public and governments about the normal operations, expectations, limitations, and emerging uses of 6G systems.
- Understand that future attack vectors will be inextricably linked to privately controlled and operated critical infrastructure.

- Explore and plan for control dynamics with 6G systems in place. For instance, NATO will likely not be able to exert “top-down” control over 6G technologies. Only a global consortium of public, private, and government actors will be able to secure critical infrastructure on the scale of a 6G roll-out.
- Balance technological determinism and tech arms race with human-centric approaches. The complexity and speed of tech innovation also means that consequences are likely to be unpredictable. Therefore, considerations outside of tech need to be integrated into planning and execution.
- Develop relationships that enable resilience, including government partnerships with entities not part of the military instrument of power.
- Train within the 6G environment to develop resilience through recovery. Plan on 6G systems failing, so practice warfighting under degraded conditions and with analog backups until planned 6G system(s) can be repaired.
- Foster adaptability in 6G system roll-outs, including addressing problems of racism, ethnic tensions, violence, social equity, and commitment to victims who are expected to be attacked through 6G systems.

Although the intention of Threatcasting is to forecast a dark future, the method is ultimately designed to prepare for undesirable futures and identify actionable steps to prevent, mitigate, and recover from them. Through this process, hope is the focal point and emerges through proposed actions.

Threatcasting analysts frequently turn to poetry to illustrate both the dark complexity of situations expected in the future and the strength derived from responding to them effectively.

In a realm of 6G, future unfolds,  
Humans and machines, a story to be told.  
Together they work, a powerful blend,  
But dangers lurk when trust we suspend.

Algorithms soar, devoid of emotion's grace,  
Craving human insight to navigate in space.  
Let's blend our gifts, harmonize in tune,  
For a future of strength, not of sand too soon.

In partnership strong, we conquer each strife,  
Guiding the future, hand in hand, in life.  
Human touch, a guiding light we embrace,  
Shaping a world of boundless grace and space.

With synergy's dance, we forge a new way,  
Unlocking potential, a radiant display.  
Through collaboration, we chart the unknown,  
A future where trust in both is truly sown.

- ChatGPT, using GPT 4.0, 2023

### **WHY THIS POEM MATTERS**

This poem is significantly relevant, as in 2023, ChatGPT, a current application of artificial intelligence technology, was used as a tool to portray this future and generate this "creative" poem.

As a predominately western-based society, the country and its partners find themselves teetering on the edge of a foreboding precipice. Given that, all participating parties must be thoughtful and intentional about how they proceed for fear of missing potential innovations, while at the same time falling victim to possible hazards.



# Introduction

Science fiction books and movies condition society to prepare for the advent of artificial intelligence (AI) and a hyper-connected world. Visions of advanced technologies, augmented realities, robots, and even robot uprisings have captivated audiences for decades. With this, society racing towards a future to achieve an advanced civilization – a harmony of human-machine teaming and interactions intertwined into every aspect of life. It is easy to gravitate towards the extreme when considering the potential outcomes, by either focusing on the utopian, best case scenarios, or by considering the extremely negative consequences, where one descends into a dystopian future.

This report considers the inevitable balance that will exist between different facets of these two extremes. It presents the reader with an analysis of how many different variables – positive, negative, and neutral, might interact with one another to create the future in which 6G systems are ubiquitous and ever-present. While the Threatcasting model is used to describe futures that are rife with turmoil and chaos, this study offers new observations that have yet to be seen in previous Threatcasting events and reports. The central findings of this report illuminate how remarkably passive the human condition is in surrendering their privacy for the sake of progress as well as some of the consequences of doing so.

In many ways, 6G promises to serve as the catalyst to the utopian world that science fiction has conditioned western society to envision and pursue. As such, subject matter experts (SME) and workshop participants effortlessly described futures in 2030 where 6G has fully permeated human lives. However, a paradox emerged where the journey to achieve this connected state further isolated humans, and came at a cost of privacy and increased vulnerabilities. More astoundingly is society's apparent ignorance of these risks. In short, while 6G may not generate unimaginable technologies, there is a toxic side of humanity that is not being recognized, while it is simultaneously surrendering its power. It is the proclivity of business to optimize for profit to manage optics and satisfy shareholders. Although society has been fueling this behavior, the

time has come to advocate for transparency, security, and privacy from companies who are creating these technologies. This fuels hopes to achieve a utopian future without irrevocably giving away all security and privacy to do so.

## ANALYST STATEMENT

This report suggests that a path to 6G has been under development for some time, but it also seeks to articulate awareness and intervention of blindly following that path on a global scale. The goal is to advise the United States and NATO in key areas, rather than provide an all-encompassing assessment of 6G technologies. Central to these key areas is an understanding that the modern battlefield is now the entire planet. Future conflicts will likely not be in large vacant areas. They are expected to be in heavily populated areas, as is demonstrated, for instance, by the Ukraine-Russia conflict.

As a result, streets, homes, and everything connected together are now potential targets. Commercial technologies are woven into the modern battlefield and inherently bringing businesses alongside them. This hyperconnected battlespace of military and civilian technologies exponentially increases the complexities of targeting, especially when discerning “friend from foe” within the information environment. NATO, Russia, and the future of the Taiwan-China relationships will be imbued with these intricacies. 6G will amplify these complexities. It must be discussed now to navigate a global environment that works both for and against NATO.

## 6G Overview

The sixth generation (6G) of wireless technologies is defined in this report as the catalyst to the next evolution of an interconnected world that fuses humans with machines and enables revolutionary changes to society. Achieving 6G will depend on five key physical components:

- At least terabit-per-second data transfer speeds.
- Terahertz signal transmission, with wavelengths approximately 3 micrometers long.
- Precision location services.
- Intelligent network controls.
- Increased network reliability.

### Workshop Definition of 6G

The sixth generation (6G) of wireless technologies is the catalyst to the next evolution of an interconnected world that fuses humans with machines to enable revolutionary changes to society. This is achieved through:



1 Terabit/sec  
Speeds



Terahertz Signal  
Transmission



Precision Location  
Services



Intelligent Network  
Controls



Increased Network  
Reliability

To put this into perspective, 6G technology is intended to be nearly 100 times faster than 5G.<sup>2</sup> This would be the equivalent of uploading a 20-terabit file in approximately 16 minutes on 5G, compared to 20 seconds on 6G. The combination of these components will generate and move vast amounts of data that will transform how society operates. With the ability to compute data on endpoint devices rather than on large servers with the ability to transmit it with extremely low latency, 6G systems create numerous possibilities for how people can interact with machines and with others.

### Wireless Evolution



1G  
Cellular  
Calling



2G  
Messaging  
Capabilities



3G  
Internet  
Access



4G  
Apps &  
Streaming



5G  
Cloud &  
IoT



6G  
Fully  
Connected

<sup>2</sup> Bernard Marr, "6G Is Coming: What Will Be The Business Impact?," *Forbes*, (June 28, 2023). <https://www.forbes.com/sites/bernardmarr/2023/03/17/6g-is-coming-what-will-be-the-business-impact/?sh=7819b2062f10>.

# Introduction to the Threatcasting Method

Threatcasting is a method used to help multidisciplinary groups envision and plan for future scenarios. It is a particularly powerful method in the national security space that ties a specific research area - in this case, the threat of 6G systems - with an emphasis on both preemptive action and post-event recovery. It is also a process that enables systematic planning against threats up to ten years in the future. Utilizing the Threatcasting Method<sup>3</sup>, groups explore possible future threats, how to mitigate them, and build the future they desire. Information obtained through this process provides organizations and decision-makers with a framework to plan, prepare, and make decisions in complex and uncertain environments. Since the Threatcasting Method mimics reality with science-fiction based models that are backed by science and Subject Matter Expert (SME) interview data, it often guards against strategic surprise. Because of this, when a crisis occurs or an opportunity presents itself, a decision-maker or a leader is also better prepared. Their response is more likely to be, "We have imagined and discussed this before. We know where to start..."

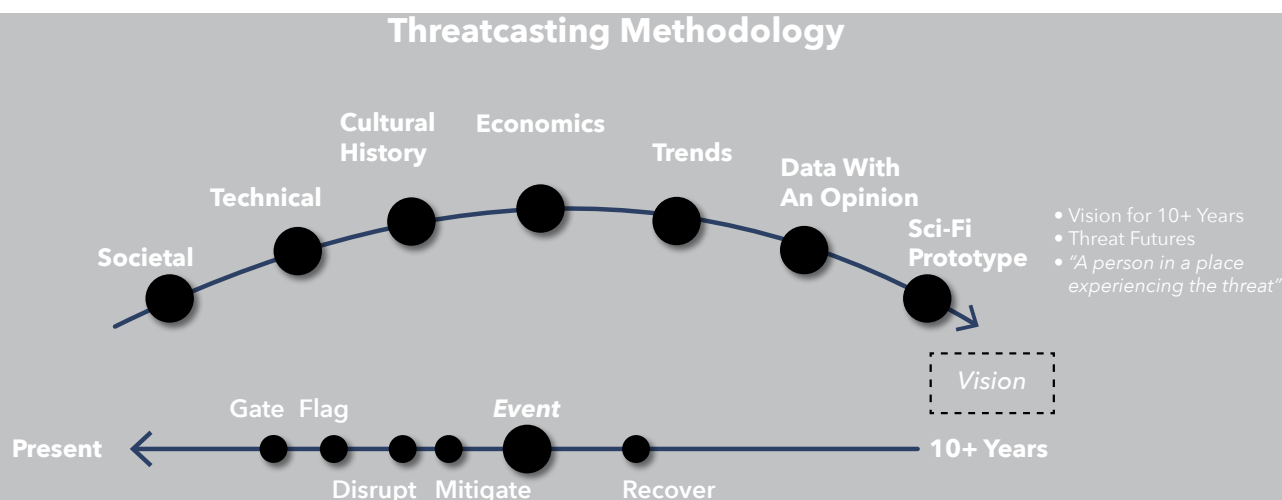
Threatcasting is a continuous, multiple-step process with comprehensive inputs. These inputs range from social science, technical research, cultural history, economics, and trends analysis. Expert interviews, sometimes called "data with an opinion," and

science fiction storytelling carefully shape inputs and trends that attempt to illustrate the research question scenarios. This dynamic set of inputs inform the exploration of potential visions of the future.

To address the topic of this report, a cross-functional group of practitioners gathered for two days in April 2023 in Norfolk, Virginia. They explored the future of 6G wireless communications as well as their implications for NATO allies. Participants reflected on research inputs from a diverse data set that included SME interviews (see Appendix A). They then synthesized the data into workbooks and conducted four rounds of Threatcasting exercises. The purpose of the exercises was to develop effects-based models, each with a person in a place, experiencing their own version of a threat.


After the workshop concluded, the research team methodically analyzed the scenarios to categorize and aggregate indicators of how the most plausible threats could materialize during the next decade.

The team also considered implications for NATO to mitigate the threats. These implications are aligned to NATO's strategic vision of "Outs" and include recommendations to the people, organizations, and processes that have some level of control over the resources and decisions that coincide with naturally occurring and adversary-driven events.



3 Brian David Johnson, Natalie Vanatta, and Cyndi Coon, *Threatcasting* (Morgan and Claypool, 2021), i-285.





**Threatcasting explores future scenarios, then systematically works backwards to disrupt or prevent futures we want to avoid, and to create the future we need.**

To that end, there are a series of indicators (“flags”) worth watching out for, typically outside of NATO control. These flags are paired with actions to effectively disrupt, mitigate, and recover from potential vulnerabilities as they develop into threats. For this report, these actions are framed within the six “Outs” with additional commentary on their respective implications. It is important to note that the exploration of indicators and actions are based exclusively on the Threatcasting research questions, so therefore, do not fully represent all possible and plausible threats.

Using the Threatcasting Method, participants identified the beginning of a set of plausible threats and external indicators. They then recommended actions that, if taken, are expected to mitigate the threats. While not definitive, this process provides participants, readers, and organizations with a starting place, so they are able to consider how future threats might manifest in certain contexts and how to address them.

# What is the Threatcasting Foundation?

The Threatcasting foundation consists of the primary topic, research question, and applications area that will be covered by the Threatcasting Method as well as how the output is to be used. Establishing a robust, researched, and focused foundation is an important skill for any research project. The better defined the foundation, the more efficient and effective the application of the Threatcasting method will be.

In this report, the authors examine future threats from 6G technology advancement and use, particularly in military applications. The research question, “What are future threats to government, military, and critical infrastructure from attacks carried out on 6G communications systems?” allows the U.S. and NATO allies to investigate the next generation of critical communication systems that will drive military instrument of power in future competition and conflict.

## Foundational Research Question:

“

**WHAT ARE FUTURE THREATS TO GOVERNMENT, MILITARY, AND CRITICAL INFRASTRUCTURE FROM ATTACKS CARRIED OUT ON 6G COMMUNICATIONS SYSTEMS?”**

As such, this project seeks to:

- Advance the understanding of novel attacks on government, military, and national critical infrastructures.
- Develop a definition on what 6G systems are.
- Define 6G applications that NATO may need to understand, adopt, or prepare countermeasures for.
- Explore new logistics and supply chains for 6G systems, especially data supply chains from high volume and high-density sensor systems.
- Envision critical latency intolerant applications, such as remote medicine in combat environments.
- Understand data-dense environments, such as the Internet-of-Body-Things, the Internet-of-Battlefield-Things, and other applications that range from personalized health to large-scale networked industrial control sensors and safety systems.
- Envision military operations being augmented by artificial intelligence, including the possible advances in edge computing and decision mechanisms for lethal autonomous weapon systems.
- Examine emerging data streams, such as biometrics that provide haptic feedback for human-to-human, human-to-machine, or machine-to-machine interfaces.

## APPLICATION AREAS

This research includes recommendations for military, government, and private actors to take to avoid, mitigate, and recover from trends leading to undesirable futures. Beyond direct applications to NATO and the U.S. Army, other affected government organizations (e.g., Federal Communications Commission, National Telecommunications and Information Administration, Cybersecurity and Infrastructure Security Agency, International Telecommunication Union), military departments and offices (e.g. U.S. Space Command, Army Futures Command, Service Spectrum Management Offices, U.S. Army Intelligence and Security Command), and critical infrastructure operators and supervisors (including industry actors) will benefit differently from the findings and implications from this report. Threats that emerge from 6G systems will create different risk profiles and different responses for each entity.

Some questions that individual organizations may wish to consider as they apply the findings from this report include:

- How might the adversary deny, degrade, deceive, disrupt, and/or destroy my access and control over my 6G system?
- How might my organization counter, disrupt, mitigate, and/or recover from a perceived threat?
- What is my organization's role in achieving NATO's strategy contained in the "Outs"?



# Functional Definitions

## Introduction and Purpose

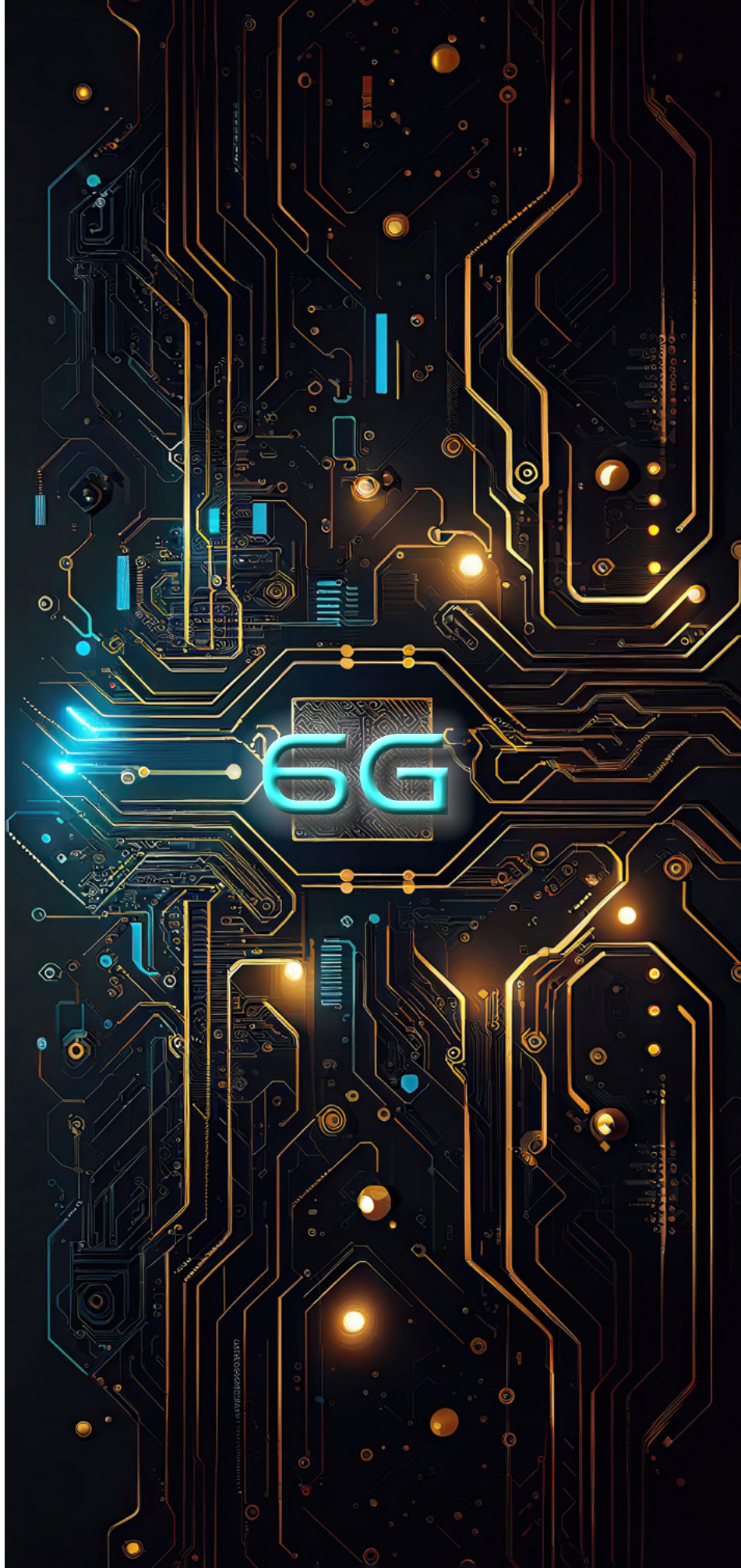
The following definitions are meant to capture key concepts used by the analysts throughout the report. Each definition is comprehensive and referenced where possible and appropriate. However, these functional definitions are not meant to be exhaustive. They are meant to capture overriding concepts that help to form the analysts' findings. Most of the definitions already exist, but some like "6G systems" are used to capture new and emerging technological and conceptual ideas.

### **6G SYSTEMS**

This report uses the term 6G systems as a concept that indicates more than the devices, antennas, and data that make up current ideas of wireless communications. For the purposes of this report, 6G systems include 6G communications networks; connected user devices; software (e.g., AI, databases, enterprise specific tools, etc.); and other environments (e.g., a metaverse of interrelated and interconnected apps, all with access to appropriate data, sensors, and processing power). 6G systems also affect the interconnectedness of humans and the social implications of the humanity that is inextricably tied to massive data and highly connected devices. The system is incomplete without the human factors.

### **VISIONS OF 6G SYSTEMS**

In addition to the concept of 6G systems (sometimes referred to as "NextG"), authors of this report acknowledge several alternate visions for the future of 6G that are impacting research and development programs within industry and the government.



Different organizations have their own way of describing the future of 6G. Five are presented for initial consideration.

1. **Ericsson:** "Scale and limitless connectivity, Privacy and Security, Cognitive Networks, and Network Compute Fabric."<sup>4</sup>
2. **Nokia:** "The role of next-generation networks is the unification of our experience across the physical, digital and human world,"<sup>5</sup>
3. **Next G Alliance:** "Six audacious goals – 1. Trust, Security, and Resilience, 2. Digital World Experiences, 3. Cost Efficient Solutions, 4. Distributed Cloud Communications Systems, 5. AI-Native Wireless Networks, and 6. Sustainability."<sup>6</sup>
4. **Department of Defense:** "The DoD has a vital interest in advancing 5G-to-NextG wireless technologies and concept demonstrations. These efforts represent our continuing investments via public and private sector collaboration on research and development for critical Beyond 5G technology enablers necessary to realize high performance, secure, and resilient network operations for the future warfighter."<sup>7</sup>
5. **Department of Homeland Security:** "5G wireless technology represents a transformation of telecommunication networks. These developments introduce risks that threaten homeland security, economic security, and other national and global interests that will continue to evolve through the transition to 6G."<sup>8</sup>

## ARTIFICIAL INTELLIGENCE

AI may be used broadly to describe the ability for computers to mimic, augment, complement, or replace functions traditionally performed by humans.<sup>9</sup> Machine Learning (ML) is one of several methods for achieving AI, but is unique in that it is reliant on data being fed into the system, then these algorithms are specifically trained to identify patterns or anomalies within that data.<sup>10</sup> ML can further be expanded into deep learning models, such as ChatGPT, that leverage a network of information to identify patterns or connections, or even make inferences about the data itself.<sup>11</sup> For the purposes of brevity, this report uses AI as an umbrella term, but acknowledges that there are nuances of AI that can further refine the "kind" of AI being referenced.

---

4 Amir Gomroki, Hala Mowafy, and Mischa Dohler, "Global and Groundbreaking! What the North American Next G Alliance Means for 6G," *Ericsson Blog*, (June 30, 2022), <https://www.ericsson.com/en/blog/2022/6/north-american-next-g-alliance-6g>.

5 Nokia, "6G Explained," (2023), <https://www.nokia.com/about-us/newsroom/articles/6g-explained/>.

6 Next G Alliance, "Next G Alliance Report: Roadmap to 6G," (February 2022), <https://roadmap.nextgalliance.org/>.

7 U.S. Department of Defense, "Three New Projects for DOD's Innovate Beyond 5G Program," (August 2, 2022), <https://www.defense.gov/News/Releases/Release/Article/3114220/three-new-projects-for-dods-innovate-beyond-5g-program/>.

8 U.S. Department of Homeland Security, "5G/6G Wireless Networks," (February 2, 2023), <https://www.dhs.gov/science-and-technology/5g6g>.

9 Columbia University, The Fu Foundation School of Engineering and Applied Science, "Artificial Intelligence (AI) vs. Machine Learning," (2023), <https://ai.engineering.columbia.edu/ai-vs-machine-learning/>.

10 Ibid.

11 OpenAI, "GPT-4," (2023), <https://openai.com/gpt-4>.

# Prompts and SME Interviews

## What are Prompts?

This section highlights several SME opinions on how 6G systems and technologies might develop over the next decade. These prompts provide research, data, and opinions about the future. They guide workshop participants and analysts to create the framework for the “art of the possible” on topic areas as well as give guidance to participants when they explored the Threatcasting research question.

Each expert provided their views on the following research question: “What are future threats to government, military, and critical infrastructure from attacks carried out on 6G communications systems?”

The scenario addressed in the Threatcasting session is the world in 2035/2040 and what new applications/capabilities will be present as a result of 6G (e.g., with its higher data rate, lower latency, better reliability, faster processing, and more complete coverage). More importantly, considerations include the applications that might become widely embraced by the military, but could be fraught with vulnerabilities. Vulnerabilities are numerous and are expected range from perfectly orchestrated supply chains, remote medicine in combat environments, and collaborative robots to internet-of-body-things, biometrics, and the sheer amount of data available to ourselves and our adversaries. Ultimately, the focus is on how these applications/capabilities might negatively and positively affect militaries, governments as well as society.

## **SUMMARY OF SME INTERVIEWS**

6G technology presents unique challenges and opportunities. For friendly alliances, 6G offers faster speeds and lower latencies, that also enable efficient command-and-control communication, rapid distribution of command intent, and intelligence products. However, it also poses defensive challenges, as current sensing technology need to evolve in order to detect higher frequency emissions.

The application of 6G in weapon systems could revolutionize combat that will, in turn, driving novel developments in advanced sensing capabilities and cyber defenses. 6G’s impact on law enforcement raises concerns about effective system management, misuse, and privacy abuse. The technology also has implications for governance, which would potentially strain the relationships humans have with one another and exacerbating existing societal divides.

As 6G is embraced, responsible technology deployment and equitable access are crucial. The predicted capabilities of 6G, offer revolutionary possibilities, but also demand careful risk management, particularly regarding cybersecurity and privacy. Strategic national efforts and stakeholder collaboration are needed to address societal and economic needs in the transition to NextG technology. The economics of the wireless carrier business are driving a shift towards “softwarization” and reliance on internet packet format data. In addition, complex systems and the Internet-of-Things (IoT) introduce security challenges.

In a 6G world, power dynamics may shift, and attackers could pose significant threats by gaining control of edge devices with advanced computing or AI-on-devices. It’s also important to prepare for the transformative era of space technology, leveraging next-generation communications like 6G for enhanced battle management and situational awareness, while considering new strategies for “informatized warfare”.



## **SPEAKER A - DR. RICHARD WITTSTRUCK**

- 6G technology will provide Blue Force with advanced communication abilities, offering higher operational speeds, frequencies, and lower latencies - transforming real-time command and control procedures.
- Red Force, on the other hand, will face challenges due to 6G's high frequencies that disrupt current sensing technology, necessitating new investment strategies for sensing and responding to these emissions.
- To navigate the 6G era, we must develop new sensing capabilities for higher frequencies, create new data processing algorithms, and ensure protection against counter-6G technologies - also to leverage artificial intelligence and machine learning.

## **SPEAKER B - BOB HARRISON**

- 6G technology, marking the transition from an Internet-of-Things to a network of intelligence, could revolutionize various fields, including policing, where AI can help consolidate inputs from various sources into a single document, which also improves efficiency and public safety.
- Despite the potential benefits, the rise of 6G and AI brings with it various societal challenges, such as increased social isolation and potential misuse, which demands human and technological constraints to ensure optimal use without opening threats that can be exploited.



### **Dr. Richard Wittstruck**

6G technology empowers Blue Force with advanced communication abilities, but Red Force faces challenges due to high frequencies that require investment in sensing technology and the development of new capabilities to navigate the 6G era.



### **Bob Harrison**

6G tech and AI has the potential to revolutionize fields by consolidating information and improving efficiency, but also poses societal challenges, such as isolation and misuse, which emphasizes the need for responsible development and promote well-being.



### **Dr. Tim Persons**

6G tech promises increased performance, which impacts warfare through enhanced remote operations, while the shift to edge computing and AI everywhere presents opportunities and risks, such as AI corruption, loss of control, and eroded privacy.



### **Dr. Tom Rondeau**

6G will revolutionize interactions with the cyber-physical world through new features like built-in AI/ML, improved energy efficiency, AR/XR services, and integrated sensing, while raising concerns about cybersecurity, surveillance, and the need to balance technology with democratic values.



### **Dr. Colleen Josephson**

We must focus on identifying and characterizing NextG social and economic drivers to prioritize digital equity, sustainability, economic growth, and quality of life, while addressing concerns regarding trust, privacy, and sustainability - in emerging tech like VR, XR, and brain-computer interfaces.



### **Dr. Jonathan Smith**

The 'softwarization' shift in 5G/6G networks brings complexity and challenges due to distributed devices, while proposals for AI-driven network operations carry risks of erroneous decisions, increased security threats, and difficulties in management strategies for defense in the IoT era.



### **Dr. Joel Mozer**

The space enterprise is rapidly growing and transforming and is protected by the Space Force. As it expands into areas like 6G communications, it requires planning for economic growth, increased human presence, and adaptation to the challenges of "intelligentized" warfare.



### **Dr. Ang Cui**

Control of bandwidth and resources has shifted towards attackers due to insecure devices at the network's edge. This leads to concerns about widespread manipulation and deep fakes as well as the criticality of securing these devices to prevent adversaries from gaining control over critical resources.



### **Anton Monk**

Narrowband spectrum and satellite systems improve soldier communication on the battlefield, but implementing secure messaging and IoT applications in space requires coordination, sustainability, and seamless connectivity in 6G.



### **Michelle McClure**

The transition to 6G networks will bring faster speeds, increased capacity, advanced AI capabilities, and improved integration, while requiring new security approaches to counter threats and ensure network integrity - despite the potential for new attack vectors like deep fakes and quantum manipulation.

- As we move forward with 6G and AI technologies, we must actively engage in shaping their development and application to ensure they enhance our capabilities and improve society, rather than isolate individuals and exacerbate societal divisions.

### **SPEAKER C - DR. TIM PERSONS**

- 6G, expected around the mid-2030s, could deliver true presence-like technology with vastly increased performance and data rates, profoundly impacting areas like warfare by enabling users to have full sensory awareness in remote operations.
- The shift from core to edge computing will be amplified with 6G, which means AI everywhere - bringing with it both opportunities and risks, such as potential AI corruption or edge computing hijacking, which will also lead to loss of control and situational awareness.
- Due to the enormous amounts of data 6G could handle, it may offer full location awareness across all four dimensions, which will potentially lead to super-precise tracking and intelligence collection, but also a complete eradication of privacy as we know it today.

### **SPEAKER D - DR. TOM RONDEAU**

- By 2035, the sixth-generation mobile system, 6G, will provide new capabilities, such as built-in AI, improved energy efficiency, AR/XR services, global connectivity, integrated sensing and networking, as well as hyper-localization services that will result in new ways of interacting with the cyber-physical world.
- 6G's advancements, built upon the groundwork laid by 5G, could lead to innovative technologies, such as AR/XR capabilities in everyday devices, remote medicine, automated traffic controls as well as secure supply chains, and highly capable intelligent agents that will transform many sectors, including warfare.
- However, these developments also bring significant drawbacks and concerns, including cybersecurity risks, potential for ubiquitous surveillance, and the need for balancing technology with democratic values. This requires the investment in technologies, policies, and practices to minimize threats and educate users about them.

### **SPEAKER E - DR. COLLEEN JOSEPHSON**

- The Societal and Economic Needs working group is working on identifying and characterizing the NextG (next-generation wireless communication technology) social and economic drivers, with a focus on digital equity, trust, and sustainability as well as economic growth and quality of life.
- Issues of trust and privacy are paramount with new technologies, such as VR, XR, and brain-computer interfaces becoming more prevalent, as they handle high-sensitivity information, which, if mishandled, could lead to invasive insights into American citizens and institutions.
- Sustainability is a crucial consideration for NextG systems, as the growing impact of the technology sector on climate change necessitates a shift towards environmentally conscious design and operation. This is in addition to the necessity to drive economic growth and enhance quality of life through innovation and improved public services.

### **SPEAKER F - DR. JONATHAN SMITH**

- The shift towards 'softwarization' in 5G and 6G networks brings about complex software that will be running on many devices close to the edge of the network. This will offer high throughput, but will also result in greater control and maintenance difficulties that are due to geographical spread.
- Proposals are being made for AI to manage network operations, using machine learning, but there are inherent risks, including the potential for the AI to make erroneous decisions that are based on the data it has processed. This will potentially result in significant threats.
- The advent of the IoT increases the diversity of device types and software and adds to the complexity of the system. Thus the potential for security risks is heightened, especially in the context of defense, where adequate configuration management strategies for 6G networks might be hard to implement.

### **SPEAKER G - DR. ANG CUI**

- In a potential 6G future, the bandwidth under control by defenders (good actors) has significantly shifted towards being under the control of attackers (bad actors) - primarily because of insecure devices on the network's edge.
- This shift in control could also extend to compute resources that will result in attackers having a greater capacity for machine learning and AI than defenders, leading to potential issues, such as widespread deep fakes and manipulation of perceived reality.
- The success of a secure 6G world is dependent on who controls the devices on the edge of the network; if we cannot ensure control and security of these devices, we risk handing over critical resources to adversaries.

### **SPEAKER H - DR. JOEL MOZER**

- The space enterprise, driven by advancements in technology and the involvement of visionary industrialists, is rapidly growing and transforming, while the Space Force is tasked with protecting U.S. interests in this domain, which includes future expansion into areas like 6G communications and smaller, more capable microelectronics.
- Future scenarios for space include significant economic growth, expected to reach four trillion dollars by 2035, and increased presence of humans and various entities. This requires us to plan for an expanded future and address new challenges associated with increased access and activities in space.
- The hyper-connected world of the future, with access to more real-time data than ever before, will not only increase the Space Force's ability to support battle management and space situational awareness, but also requires us to leverage large data sets and AI techniques in order to reduce or eliminate the fog of war effect, and adapt to the challenges of this new era of 'intelligentized' warfare.

### **SPEAKER I - ANTON MONK**

- The use of narrowband spectrum for messaging and voice on the battlefield can significantly improve communication and situational awareness. It can also be supported by both GEO (geosynchronous orbit) and LEO (low earth orbit) satellites - with GEO solutions already available and LEO still evolving.
- Direct-to-device messaging and IoT applications in battlefield environments require careful attention to security and quality of service as well as the possibility of integrating standards-based security through devices that are small and cheap enough to be used widely, without attracting adversary attention.
- The challenges associated with implementing 5G in space include managing space sustainability, avoiding potential collisions, and effectively regulating space use. These all will be essential in coordinating security between various networks on the ground and in space - to leverage commercial solutions for defense applications, and ensure seamless connectivity through hybrid networking.

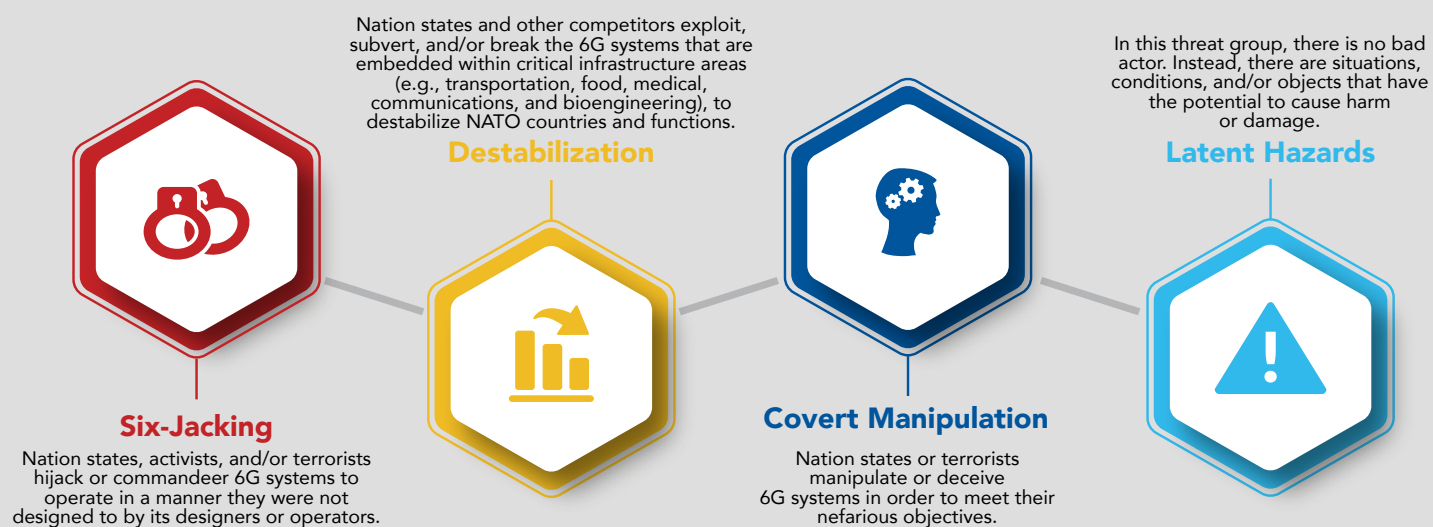
### **SPEAKER J - MICHELLE MCCLUER**

- The transition to 6G networks from 5G is expected to bring faster speeds, increased network capacity, advanced AI capabilities, and better integration across various communication channels.
- The evolution to 6G will also necessitate new approaches to security, including novel authentication, encryption, and access control, as well as communication and threat detection systems - particularly due to the larger and faster network environment.
- While 6G might open new vectors for attacks, including advanced deep fakes and manipulation through quantum aspects, the same advanced technologies will also be tools for defending against threats and ensuring network integrity.

# Findings

## What are Findings?

After the completion of the workshop and the generation of the raw data, the next phase in the Threatcasting Method is post analysis. In this phase, the data is synthesized, reviewed, and processed to develop a set of findings (i.e., possible and potential futures). This section of the report introduces four novel findings that were identified across the range of workshop models.



## FINDING #1: SIX-JACKING AS A NOVEL TACTIC DURING COMPETITION AND CONFLICT

Six-jacking is a colloquial term penned during this analysis. It occurs when nation states, activists, and/or terrorists commandeer 6G systems to operate in a manner they were not designed to by its designers or operators. In these cases, the 6G system is still functioning, but someone else has taken control of the system (in whole or in part) to point it in a different direction, using it for their advantage. Similar in context to hijacking a vessel in transit, six-jacking refers to this act within the 6G ecosystem.



By far, the most instantiated concept brought forward during the workshop, six-jacking seeks to exploit our overreliance on 6G systems to achieve ulterior motives. These motives could range from creating disorder and fomenting social unrest through mis/disinformation to manipulating remote surgical systems to assassinate individuals. This would medically harm soldiers by altering biometric controls, or even enable the performance of intelligence and information gathering. There are no shortages of potential nefarious actions that could be imposed on the population in a hyper-connected world. Tailored algorithms seeking to perfect AI systems fuel data collection of individuals and ultimately incite opportunistic behaviors to exploit these connections.



The ability to mitigate these vulnerabilities requires that the U.S. and its allies calculate a balance of openness in inviting these 6G systems into their lives along with employing the necessary security controls. However, we may already be on the path to integrate these devices. In 2021, the worldwide smart home grew by 11.7% and is projected to sustain this growth through 2026.<sup>12</sup> Billions of devices are infiltrating western society, which inherently build the foundation for six-jacking. Unfortunately, security standards will only begin to be enforced on these devices in late 2023.<sup>13</sup> There is a substantial amount of effort needed to reduce the potential for six-jacking, especially by educating the population on the challenges and opportunities of these 6G systems.

## **FINDING #2: OVER-RELIANCE CREATES LATENT HAZARDS**



Due to the current ubiquitous data collection, the future of privacy may begin to shift to discussions on ethical algorithms, data sharing, and “passive” participation on unfamiliar networks. Anonymity is highly valued by individuals, but this is

often counter intuitive to effective algorithms, which are continually being fed and are refining data about users. Although attempts to redact sensitive data may be built into some algorithms, “reidentification” may occur through the fusing of multiple algorithms.<sup>14</sup> The synthesis of this data can link seemingly benign information about an individual

with highly personal and sensitive data. This evolution of the privacy discussion further expands into “passive” network participation. An example of “passive” network participation would be Bluetooth trackers hidden in shelves to geolocate a shopper’s position in a store, which is then used to target them with advertisements about near-by products.<sup>15</sup> From an operational security perspective, similar situations are already being observed where “passive” data is being shared on fitness tracking devices that show jogging routes of users. In several instances this has inadvertently revealed the perimeter of military bases.<sup>16</sup>

IoT devices will likely comprise a large portion of 6G networks; therefore, AI-guided network management of these devices will become essential.<sup>17</sup> Consequently, device identification and device integrity with robust security and protection continue to be a challenge for IoT devices. One way to authenticate users’ devices may be through ‘fingerprinting’ devices, based on their unique hardware variations in radio frequency, signal amplifiers, or the way they convert these signals to be read by a machine.<sup>18,19</sup> Augmented by deep learning (i.e., AI), these subtle idiosyncrasies of each device could be used as a method of authentication.<sup>20</sup> Although potentially valuable to network management and security, these concepts may further the complexities of latent hazards and privacy through the tracking of both individuals and the devices they use.

12 “Worldwide Smart Home Devices Market Grew 11.7% in 2021 With Double-Digit Growth Forecast Through 2026, According to IDC,” *Business Wire*, (April 25, 2022), <https://www.businesswire.com/news/home/20220425005273/en/Worldwide-Smart-Home-Devices-Market-Grew-11.7-in-2021-With-Double-Digit-Growth-Forecast-Through-2026-According-to-IDC>.

13 “In 2023, Security-Focused Regulations and Standards Will Be Shaping IoT Device Design,” *Wireless Communications Alliance*, (February 20, 2023), <https://wca.org/in-2023-security-focused-regulations-and-standards-will-be-shaping-iot-device-design/>.

14 Vern McKinley, “The Ethical Algorithm,” *Cato Institute*, (September 14, 2020), <https://www.cato.org/regulation/fall-2020/ethical-algorithm>.

15 Michael Kwet, “In Stores, Secret Bluetooth Surveillance Tracks Your Every Move,” *The New York Times*, (June 14, 2019): sec. Opinion, <https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html>.

16 Richard Pérez-Peña and Matthew Rosenberg, “Strava Fitness App Can Reveal Military Sites, Analysts Say,” *The New York Times*, (January 29, 2018): sec. World, <https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html>.

17 Nagender Aneja et al., “AI-Enabled Learning Architecture Using Network Traffic Traces over IoT Network: A Comprehensive Review,” *Wireless Communications & Mobile Computing 2023* (January 1, 2023), <https://doi.org/10.1155/2023/8658278>.

18 Ibid.

19 Tong Jian et al., “Deep Learning for RF Fingerprinting: A Massive Experimental Study,” *IEEE Internet of Things Magazine* 3, no. 1 (March 2020): 50-57, <https://doi.org/10.1109/IOTM.0001.1900065>.

20 [https://ece.northeastern.edu/fac-ece/ioannidis/static/pdf/2020/J\\_Jian\\_RFDeepLearning\\_IoT\\_2020.pdf](https://ece.northeastern.edu/fac-ece/ioannidis/static/pdf/2020/J_Jian_RFDeepLearning_IoT_2020.pdf)

These examples represent a handful of latent hazards that have the potential to cause harm simply by their existence within the 6G systems that are woven into daily lives. The aggregation of data collection, connection, and dissemination serve as “the trifecta” of latent hazards. Unfortunately, these are the fundamental goals of 6G systems – data collection, connection, and dissemination. Moreover, less security on edge devices may inherently “bake-in” vulnerabilities from the start and set the right conditions for nefarious actors to act on these latent hazards. Although many of these challenges exist today in 5G and below technologies, the omnipresence of 6G systems may bring the significance of the situation to the general public.

### **FINDING #3: 6G SYSTEMS ENABLE DESTABILIZATION**

Primed by reliance on 6G systems, nation states may seek to exploit, subvert, or break into these systems to destabilize the nation. Destabilization can occur through many methods, but it is the predominance of attacks utilizing disinformation and attacks against critical infrastructure that were the most common sources of destabilization in our data. The objective of using disinformation is to divide, polarize, and isolate individuals, groups, and/or societies, especially to radicalize and incite violence.<sup>21</sup> Destabilization through effects imposed on or through critical infrastructure can equally disrupt political stability, social trust, military force projection.



Furthermore, it can disrupt a nation’s ability to sustain basic needs through supply chains, and/or power and water systems. Of these areas, supply chains represent some of the most vulnerable attack surfaces. Some attempts like these are already being observed. Design, manufacturing, and logistical transportation processes are actively being targeted to compromise the quality, authenticity, and/or security of supplies, which span from commercial, industry, and military consumers.<sup>22</sup>

At each stage in these processes (design, manufacturing, and transportation), 6G systems will be integrated to augment operations and oversight. AR/VR/XR systems with ‘digital twins’ aid distributed teams design and the management of programs and products. IoT devices woven into manufacturing processes will be essential for monitoring equipment status, temperatures, image processing, and data collection. Radio frequency identification tags will guide logistical operations to provide near-real-time inventory updates and shipping timelines. Each stage will be flooded with 6G systems in order to accelerate timelines and increase efficiency.

However, vulnerabilities in network design, security, and oversight may ultimately create an opportunity for nefarious nation states to exploit these areas. Manipulation of food supply chains that induce intentional delays could spoil food before delivery. Coordinated disinformation campaigns are likely to be used in order to weaken society’s trust in their government to supply and protect food sources. The fact that critical vulnerabilities and ‘backdoors’ are hidden in design processes to be exploited at a later date, make militaries and governments vulnerable. A cascading series of these events could set the conditions for a military coup, political/regime change, or invasion that would, in turn, potentially destabilize a nation.

21 Carlos Diaz Ruiz and Tomas Nilsson, “Disinformation and Echo Chambers: How Disinformation Circulates on Social Media Through Identity-Driven Controversies,” *Journal of Public Policy & Marketing* 42, no. 1 (January 1, 2023): 18-35, <https://doi.org/10.1177/07439156221103852>.

22 Jay Town, “China Exploiting Supply Chain Vulnerabilities,” *National Defense Magazine*, (December 9, 2020), <https://www.nationaldefensemagazine.org/articles/2020/12/9/china-exploiting-supply-chain-vulnerabilities>.

## **FINDING #4: 6G SYSTEMS CREATE OPPORTUNITIES FOR COVERT MANIPULATION**

Covert manipulation occurs when nation states or terrorists deceive 6G systems to achieve their nefarious objectives through unobservable methods. To the operator, these influenced 6G systems appear to be functioning correctly. It is only later that they realize there is a problem. Therefore, the manipulation is performed within a layer that is not obvious or viewable by the operator.



Covert manipulation differs from six-jacking in that during a manipulation attack, the system still performs as intended or designed, whereas six-jacking modifies the system to do something unintended. This ability to subtly manipulate the system has the potential to incite serious damage and consequences. Complacency and overreliance condition humans to accept the data 6G systems show them. But when that data can be covertly manipulated, the operator is primed to make decisions s/he believes is correct. The objectives behind covert manipulation could include achieving geopolitical gains, conducting intelligence gathering, and undermining trust in critical infrastructure as well as enabling terror acts, creating conditions for bad military decision making, and weakening military effectiveness.

Defending against these attacks is perhaps the most difficult of all. The only ways to mitigate these threats may be focused attention on nominal system performance, combined with impenetrable security. Unfortunately, security standards are lacking, and users may delegate menial tasks to AI, so they perform more complex actions - human attention to nominal performance is likely already reduced. The best safeguard may also include a hybrid approach that embeds multiple independent systems into the decision-making processes. This approach is not infallible as attackers could manipulate each independent system, but it does increase the complexity and dependency to do so.

## Discussion

### 6G Systems - External Risks

“

A STRANGE GAME. THE ONLY WINNING MOVE IS NOT TO PLAY. HOW ABOUT A NICE GAME OF CHESS?”

- *WarGames*, 1983

### IMPLICATIONS OF 6G SYSTEMS

The use of higher radio frequencies in the electromagnetic spectrum is an anticipated requirement to support 6G data throughput with minimal data latency. Consequently, these higher radio frequencies are subject to signal quality degradation and will require more devices at closer intervals to maintain the necessary speed and quality of service.

To put this into perspective, consider the number of devices required to operate 6G systems when the current technology transmit distances range from only 100 to 320 meters<sup>23</sup> - approximately the length of only two Olympic-sized swimming pools. This results in a massive proliferation and footprint of 6G devices, receivers, supporting hardware, all of which increase the electromagnetic footprint of 6G systems. Moreover, this design inherently increases substantial risks, especially in terms of network operations and security.

6G systems are projected to be ubiquitously operating and sharing data as part of a federated network. Federated networks may be designed to be “flat” - with each endpoint device independently reaching into cloud resources outside the structure of centralized control mechanisms.

Control of these systems, and most importantly the data they are sharing, requires a highly complex enterprise, with computing resources pushed to the “edge” of the network to process data.

Edge computing reduces the need to send data to massive server farms, for example, to perform calculations, which save time processing data. Access to cloud storage and robust edge computing are hallmarks of early 6G systems. However, this approach often has less oversight and control on edge devices, which are typically inexpensive, small, and may lack robust security standards. Put simply, these characteristics of 6G systems may be an ideal attack vector for criminal actors to exploit these vulnerabilities.

The mass proliferation of these attack vectors presents significant challenges, from detecting and protecting to attacks and/or exploitation. To clarify, it is important to note that current 5G and older communication systems may already be vulnerable to attacks and exploitations. However, the implementation of 6G creates a unique challenge: to compensate for the physics-related limitations of 6G, the number of edge connections must substantially increase. This greater number of access points (or attack vectors) may, in turn, provide more opportunities for harmful intrusions.

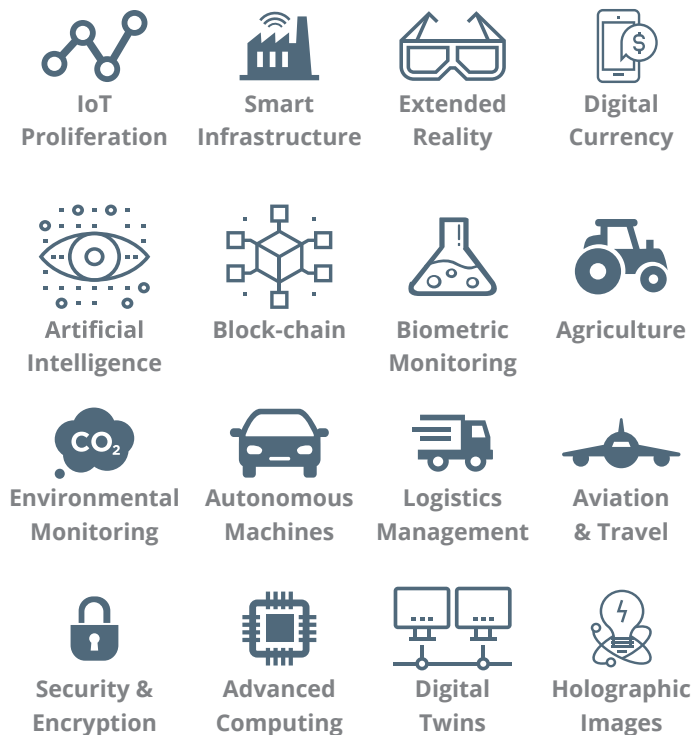
Moreover, a 6G system with ubiquitous access points may facilitate a “hyper-polar” system, where global power dynamics can dramatically shift. In this 6G system, traditional, nation-state and “terrorist” actors have an excess of access points, which ultimately levels the “entry-fee”, while simultaneously challenging traditional source identification and intent.

This low barrier to entry increases the likelihood of employment of advanced capabilities, which can enable the hyper-polar threat environment and create complex strategic challenges that must be addressed in future planning activities.

23 “LG Showcases Leadership in Next-Gen 6G THz Band Demonstration,” LG Newsroom (blog), September 14, 2022, <https://www.lgnewsroom.com/2022/09/lg-showcases-leadership-in-next-gen-6g-thz-band-demonstration/>.



## Anticipated 6G Applications



These multiple attack vectors through unsecured edge devices will inherently question the integrity of the data. Data manipulation, network obfuscation, and/or six-jacking present unique opportunities to exploit data as well as the creators and consumers of that data. Security, authentication, and reliability are essential to safeguarding 6G users, their data, and their cognitive understanding of the data. However, the paradigms of traditional network and cellular broadband security may fall short in a federated system that is anticipated to service thousands of local devices.<sup>24</sup> Herein lies perhaps one of the greatest risks of 6G systems - knowing whether the data is legitimate or not.

Architecting and implementing a hyper-connected world may in fact be the easier part. The challenge lies in understanding these connections and the data moving between them. AI and ML are at the core of addressing this challenge, but they are not without their own risks. ML cannot work without data, and both AI and ML are inherently subjected to the algorithms that underpin their operations. The more ubiquitous our 6G systems become, the more data they enable for collection and processing. The more data fed into algorithms the more effective they may potentially become. The quality and accuracy of the data being fed into the model(s) are critically important to how ML works - this is traditionally referred to as a colloquial saying of "garbage in, garbage out".<sup>25</sup> If ML models are based on false or inaccurate data, they will produce results based on that data, which may not be what the user anticipates or desires.

Caution should be applied before fully endorsing the 6G. While commercial industries tend to race to commoditize the concept, the fact remains that physics is difficult, and no amount of monetization can change that. To clarify this statement, consider the current state of 5G technologies. Throughout many countries, 5G networks are actually slower than legacy 4G speeds.<sup>26,27,28</sup> The underwhelming advances of 5G to date, especially considering it has been available to customers for over four years,<sup>29</sup> should caution the overemphasis on 6G timelines. Applications and use cases discussed in this report are relevant and appropriate; however, technology may be the driving factor for implementations, rather than subjective dates (i.e., 2030).<sup>30</sup>

24 Lina Zhou et al., "From Artificial Intelligence (AI) to Intelligence Augmentation (IA): Design Principles, Potential Risks, and Emerging Issues," *AIS Transactions on Human-Computer Interaction* 15, no. 1 (March 31, 2023): 111-35, <https://doi.org/10.17705/1thci.00085>.

25 R. Stuart Geiger, Dominique Cope, Jamie Ip, Marsha Lotosh, Aayush Shah, Jenny Weng, Rebekah Tang, "Garbage in, garbage out revisited: What do machine learning application papers report about human-labeled training data?" *Quantitative Science Studies* 2021; 2 (3): 795-827, [https://doi.org/10.1162/qss\\_a\\_00144](https://doi.org/10.1162/qss_a_00144)

26 Alan Weissberger, "Another Opinion: 5G Fails to Deliver on Promises and Potential - Technology Blog," *IEEE ComSoc Technology Blog*, (December 10, 2022), <https://techblog.comsoc.org/2022/12/10/another-opinion-5g-fails-to-deliver-on-promises-and-potential/>.

27 A. J. Dellinger, "Feel Like Your 5G Network Is Slower Than Promised? You Aren't Just Imagining It," *Forbes*, (February 28, 2021), <https://www.forbes.com/sites/ajdellinger/2021/02/28/feel-like-your-5g-network-is-slower-than-promised-you-arent-imagining-it/>.

28 Michael Gariffo, "Why Is My 5G so Slow? Comparing the Hype to the Reality," *ZDNET*, (February 7, 2022), <https://www.zdnet.com/article/why-is-my-5g-so-slow-comparing-the-hype-to-the-reality/>.

29 Verizon News Archives, "When Was 5G Introduced?," (December 6, 2019), <https://www.verizon.com/about/our-company/5g/when-was-5g-introduced>.

30 Next G Alliance, "6G: The Next Frontier of Innovation and Investment," (2023), <https://www.nextgalliance.org/>.

## OMINOUS FORESHADOWING: LESSONS FROM STANISLAV PETROV ON HUMAN-AI COLLABORATION

Stanislav Petrov was a lieutenant colonel in the Soviet Union's Air Defense Forces, who played a pivotal role in averting a potential global catastrophe during the Cold War. On September 26, 1983, the Soviet early warning system reported the launch of five intercontinental ballistic missiles (ICBMs) from the United States. Given the tense geopolitical climate of the time, the standard protocol would have been to authorize a retaliatory nuclear strike. However, Petrov, the duty officer at the time, mistrusted the machine warning and instinctively judged the alarm to be a system malfunction. He reported it as a false alarm, a decision that effectively prevented an erroneous retaliatory nuclear attack on the United States and its NATO allies. This could further led to a large-scale nuclear war and untold destruction.

Petrov's decision highlights the critical importance of human-machine teaming. In the realm of decision-making, particularly where there are high stakes or complex situations, the combination of human judgment and machine efficiency can produce outcomes that neither could achieve alone. While machines and algorithms can process vast amounts of data and make predictions or suggestions based on that data, they lack the intuition, context awareness, and holistic understanding that are more natural to humans. Machines also lack the capacity for ethical judgment, especially in situations where the 'right' decision isn't purely a matter of factual accuracy or logic.

This event also serves as a reminder of the dangers of delegating decision-making entirely to AI systems. AI technologies have made great strides in recent years, but they are far from infallible. They can be affected by the biases inherent in their training data, their algorithms, and/or their design, which, in turn, can lead to mistakes or produce unanticipated consequences. While AI and automation can offer remarkable efficiencies and capabilities, they should complement, not replace, human judgment and decision-making.

## 6G SYSTEMS - CRITICAL INFRASTRUCTURE APPLICATIONS

Different critical infrastructure will incorporate different configurations of 6G systems. This section briefly explains potential combinations of various technologies, processes, or other components of specific critical infrastructure sectors that were identified in the Threatcasting scenarios. Note that not all critical infrastructure categories are listed simply because they were not explicitly incorporated into the scenarios. Implications to these sectors are likely to include lessons that would be useful to other sectors.

**Transportation:** In the transportation sector, a sample 6G network could include a wide variety of systems. These systems include anything from autonomous vehicles (personal and freight) traveling through the land, sea and/or air, maps and way-finding systems, and transportation infrastructure to local and national driver databases, insurance data, and law enforcement communications.

**Energy:** For the energy sector, example 6G networks can include an advanced energy management system that uses 6G wireless networks, AI, and other technologies that collect and analyze real-time data using AI algorithms to optimize energy generation, distribution, and consumption. This data can be pulled from a number of distributed energy resources, such as solar panels, wind turbines, and energy storage systems.

**Medical/Health:** In the medical/health sector, a sample 6G system could include personal medical devices on the body, in the home, or implanted as well as, medical databases, and diagnostic and lab devices. In this sector, systems can also be found in physician databases, insurance information, and remote healthcare apps and services. 6G-enabled telemedicine systems could enable doctors to remotely diagnose and treat patients using advanced sensors and robotic instruments, all connected to the high-speed 6G network.

**Bioengineering:** Bioengineers and biomedical engineers combine engineering principles with sciences to design and create equipment, devices, computer systems, and software.<sup>31</sup> For this emerging subsection of the medical and health sector, the advances afforded by 6G will have an outsized impact. 6G communications networks will allow for a massive amount of data transfer, enabling many functions of bioengineering to happen in real time. These cyber/physical systems, when combined with a sentient network will constitute a unique formation of a 6G system.

This sector will be highly regulated and monitored because its 6G systems will come into contact with and use human medical data as well as humans themselves. Due to the sensitive nature of this sector will make it a prime target for threat actors. The disruption and manipulation of bioengineering and biomedical systems holds a great potential to undermine public trust in their medical systems.

**Communications:** In the communications sector, 6G systems could enable new forms of telepresence, remote collaboration, and entertainment that will allow people to interact with each other. They will be able to do so in digital environments in new ways, such as virtual reality, augmented reality, and/or extended reality. 6G systems could also enable new forms of machine-to-machine communication and automation, with advanced sensors and algorithms used to gather and process data in real-time. This will also enable autonomous systems to make decisions and take actions with unprecedented speed and precision.

**Agriculture:** In the agriculture sector, examples of 6G systems could include crop sensors, situational awareness capabilities for crops and herds, weather data, and soil data as well as harvest and yield data, market pricing data, autonomous farm equipment. It's also expected to permeate railway and trucking information, crop and herd way stations, and warehouses.

**Supply Chain:** 6G systems affect the supply chain in that "The network of suppliers deliver products from raw materials to end customers through either an engineered or transactional flow of information, goods, and money."<sup>32</sup>

In the vast supply chain sector, 6G systems will include multiple instances of cyber physical systems. A constellation of these technologies are connected to the 6G networks with powerful sensors and access to massive collections transitive data. This will mean that the complexity of these systems will be inordinately large. By definition, supply chains themselves are already complex and involve hundreds, if not thousands of people with multiple points of infrastructure, such as factories, mining operations, and warehouses. Taken as a whole, this sector also involves multiple forms of transportation over land, sea and air that are piloted by both humans as well as autonomous technologies. The Association for Supply Chain Management states, "At a high level, supply chain touches every step from growing, mining or creating a material to responsibly managing its end of life – and all of the activities in between: sales and operations planning, new product development and engineering, risk management, corporate social responsibility."<sup>33</sup>

However, the systems themselves will greatly benefit from 6G networks, as will the products and services being transported throughout their infrastructures. The more complex the supply chain, the more it will benefit from transforming itself into a 6G system. While these systems will benefit from transforming to a 6G network with its increased productivity, transparency and security – they will also be opened up for substantial disruption. The more complex the system, the more targets of attack will exist in that system.

31 Bureau of Labor Statistics, U.S. Department of Labor, "Bioengineers and Biomedical Engineers," *Occupational Outlook Handbook*, (September 8, 2022), <https://www.bls.gov/ooh/architecture-and-engineering/biomedical-engineers.htm>.

32 Paul H. Pittman and J. Brian Atwater, eds., *ASCM Supply Chain Dictionary, 17th Edition*, (Association for Supply Chain Management, 2022).

33 Association for Supply Chain Management (ASCM), "What Is Supply Chain Management?," *Supply Chain Management* (2023), <https://www.ascm.org/scm/>.

**Military and Defense Systems:** In the military sector, 6G systems could include advanced battlefield networks that leverage AI, and other advanced technologies to enable real-time situational awareness and decision-making. A 6G-enabled battlefield network could use advanced sensors to collect real-time data on the locations, movement, and activity of friendly and enemy forces. This data could then be analyzed by AI algorithms to provide commanders with a comprehensive and up-to-date picture of the battlefield. This will enable them to make better decisions and respond more quickly. In 6G-enabled warfare, AI could even be used to enhance or replace human decision-making in military operations.

## OVERRELIANCE ON TECHNOLOGICAL SYSTEMS

Overreliance on technology is one of the greatest threats that 6G systems face. When technology replaces decision-making processes or overrides traditional social functions, it becomes a crutch that has the opposite effect of enabling humans to achieve their full potential. Overreliance on 6G systems might emerge in two ways: integration and augmentation. Each are described below.

### *Integration*

An extreme increase in participation with hyper-connected 6G systems has the potential to radically shape human-machine relationships, and subsequently, human-human relationships. High data speeds with low latency widens the aperture for many technologies, especially “presence” technologies, such as Augmented Reality (AR), Virtual Reality (VR), Mixed Reality (MR), and Extended Reality (XR). Through these technologies, the migration into the virtual world will significantly change how we interact with machines and each other.

To illustrate this idea, consider how social interactions changed during the COVID-19 pandemic. Although many were forced to adopt the virtual world, this shift may have foreshadowed life in a 6G systems world where social “norms” began to change.<sup>34</sup> Ultimately, people experienced “connectedness” based on their willingness to embrace technologies. However, this comes with challenges and opportunities depending how technologies are utilized - and for how long.<sup>35</sup> The digital world has the potential to impact everything from mental health to our ability to exercise free speech.<sup>36</sup> 6G systems may go beyond this “willing connectedness” to include even unwitting connections that morph our perceptions of each other.

For example, one workshop group envisioned a 6G systems world with AR glasses that use facial recognition to identify a person, then comb the internet to show personal facts, social media posts, and other public information about a person during a face-to-face conversation. But with the speed of 6G systems, more egregious scenarios may materialize where real-time deep fakes are employed to change the face of the person on the other side of the AR glasses. The deep fake functionality may also have the ability to change voices to a more pleasing tone, register, and/or tempo.

These examples highlight the need to educate the public on understanding the challenges and opportunities in this hyper-connected world. AI combined with the speeds and ubiquitous nature of 6G systems make these scenarios plausible and may reshape how we connect with each other - either willingly or “passively.”

Unsurprisingly, the premise of passive data sharing is already a reality. Western society is surrounded by devices that share data about personal health, such as heart rate monitors on smart watches, precision locations, as well as AI assistants operating alongside us to help us live our best lives. Privacy and operational security are present today and will only be amplified by 6G systems.

<sup>34</sup> Apurvakumar Pandya and Pragya Lodha, “Social Connectedness, Excessive Screen Time During COVID-19 and Mental Health: A Review of Current Evidence,” *Frontiers in Human Dynamics* 3 (2021), <https://doi.org/10.3389/fhumd.2021.684137>.

<sup>35</sup> Ibid.

<sup>36</sup> Ibid.



The drive to achieve this hyper-connected 6G systems world may also come with substantial environmental impacts. Many 3/4/5G cellular towers today are modified to attempt to blend into their environments. Obscure “palm trees”, “pine trees”, or even “cacti” are woven throughout our environments to attempt to conceal their footprint. Consider the physics-based challenge of 6G with its higher frequencies that require more devices and in closer proximity. Cell tower designs may be challenged due to the massive dispersion of 6G towers throughout the land. Moreover, each tower would increase the demand on the power grid, and likely create higher environmental impacts on their respective local areas.

### *Augmentation*

The augmentation of critical tasks to AI-based machines requires an immense trust that is often willingly given away. As an example, people usually trust that the articles read online were authored by a person, when in fact many are written by AI-guided programs.<sup>37</sup> People usually trust the person they are chatting with online is an actual person, when in reality it may be a highly anthropomorphized chatbot.<sup>38</sup> AI is trusted so much that in some cases, its systems are used to drive people to their destinations. Partnering with AI to increase effectiveness and efficiency may be the hallmark of the next decade, but caution must be applied when transferring critical functions to AI and implicitly trusting the results. Fortunately, some studies show a reluctance to overtly hand-over complete trust to AI, but it must be considered how to design frameworks for augmentation so as to prevent over-conditioning of trust.<sup>39</sup>

The urgency to integrate and augment 6G systems to the point of overreliance may come with a series of costs that include vulnerabilities to privacy and connectedness, security, and from an environmental perspective. More research is required to validate these hypotheses, but the observations are rooted in logic which is derived from the current status quo.

The adoption and proliferation of 6G systems may increase an over dependence on these systems; therefore, these conversations are necessary to have now in order to balance reliance and the employment of 6G.

## **EMERGENT BEHAVIORS**

Subtly nestled within society's reliance on 6G systems are current emerging behaviors on how these technologies are leveraged to interact with AI. Rather than predict “what” AI will do is, it's more important to focus on “why” use AI to begin with. At the heart of AI use is convenience and efficiency. The demand to automate mundane tasks, help in the analyzes of massive amounts of data, and aid in prediction modeling. These are both well-suited scenarios for AI. The danger occurs, however, when decision making is relegated to these 6G systems and their native AI processing. Intelligent AI algorithms today are acting on society's behalf to drive cars, fly drones, perform data analysis, and much more. It's just critical to remember the need for human validation in order to make “sense” of the contextual elements of the situation - just as Petrov did over 60 years ago.

### *Advanced Computing*

Advanced Computing is an umbrella term that covers emerging computational technology currently in development. The term can refer to both hardware and software that run on these machines. More recently, the term has expanded to include network devices and the hardware and software platforms that connect them. The term itself is intentionally nebulous, given the rapid pace of change, as technologies achieve mainstream success or fail to break through.

37 Nicole Martin, “Did A Robot Write This? How AI Is Impacting Journalism,” *Forbes*, (February 8, 2019), <https://www.forbes.com/sites/nicolemartin1/2019/02/08/did-a-robot-write-this-how-ai-is-impacting-journalism/>.

38 Crollic, C., Thomaz, F., Hadi, R., & Stephen, A. T., “Blame the Bot: Anthropomorphism and Anger in Customer-Chatbot Interactions,” *Journal of Marketing* (2022), 86(1), 132-148. <https://doi.org/10.1177/00222429211045687>.

39 Zhou, L., Rudin, C., Gombolay, M., Spohrer, J., Zhou, M., & Paul, S., “From Artificial Intelligence (AI) to Intelligence Augmentation (IA): Design Principles, Potential Risks, and Emerging Issues,” *AIS Transactions on Human-Computer Interaction*, 15(1) (2023): 111-135, <https://doi.org/10.17705/1thci.00185>.

Currently, Advanced Computing refers to, but is not limited to the following range of technologies:

- Supercomputing, edge computing, cloud computing, and new computing architectures.
- Virtual reality (VR), augmented reality (AR), mixed reality (XR), and "the Metaverse".
- Trusted authentication, disaster recovery, computer forensics, and identity management.
- Digital convergence between cyber and physical systems.
- Blockchains, "web3," shared distributed ledgers, traceability, and trustless systems.
- Neuromorphic, edge, and virtual systems.
- Artificial Intelligence (AI).

The United States Department of Defense, in its 2018 AI Strategy, defines artificial intelligence as "the ability of machines to perform tasks that normally require human intelligence - for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action - whether digitally or as the smart software behind autonomous physical systems."<sup>40</sup> In the words of computer scientist Elaine Rich, "AI is the study of how to make computers do things at which, at the present time, people are better."<sup>41</sup>

There are three main sub-categories of AI. The most common variety today is artificial narrow intelligence (ANI), in which some researchers refer to as "weak" AI. These algorithms are goal-oriented and designed to perform a specific task. The "weak" notation is misleading in that the current uses of ANI, while narrow, have proven to be robust and successful. Some of the more promising examples of ANI, include Amazon's and Apple's voice assistants, Facebook's facial recognition abilities, and OpenAI's GPT-3 and DALL-E 2 - all of which can spontaneously generate creative text and images from open-ended prompts.

Another sub-category, artificial general intelligence (AGI), on the other hand, has been dubbed "strong" AI. This is the domain of machines that learn, understand, and act in ways that are analogous to humans. They are able to think, strategize, and perform multiple tasks under uncertain conditions - without priori knowledge or by being specifically designed to perform them. AGIs do not currently exist, but predictions of their imminent arrival have been a hallmark of the field. Artificial super intelligence (ASI) is a hypothetical goal seen most often in science fiction films and novels. These are machines that have transcended sentience and are capable of genuine creativity, social skills, and wisdom.

### *Anti-fragility*

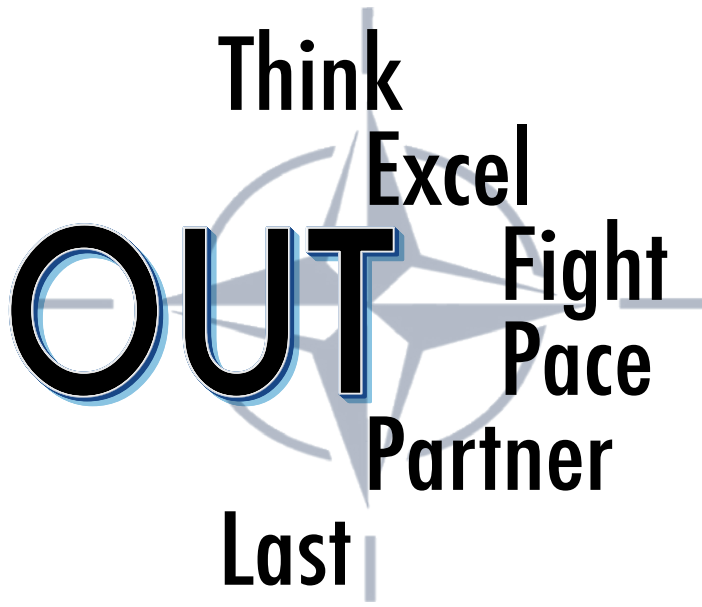
In his 2012 book, *Antifragile*, essayist, mathematical statistician, and risk analyst Nassim Nicholas Taleb coined the term "antifragile." He defines it in this way: "Antifragility is beyond resilience or robustness. The resilient resists shocks and stays the same; the antifragile gets better. This property is behind that which has evolved and survived over. Examples are the evolution of life forms, cultural norms, ideas, political systems, technological innovation, corporate survival, good recipes, legal systems, equatorial forests, bacterial resistance...."<sup>42</sup> Since 2012, Anti-fragility as a concept has been used to promote a state for organizations, technical systems, communities and even individuals to aspire to. As Taleb points out, being antifragile means going beyond just resiliency. It is a state wherein the system comprehends that there will be shocks and attacks. It is the experiences of these shocks and attacks without the failure or collapse of the system that makes it stronger.

40 U.S. Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*, 5.

41 Elaine Rich, "Artificial Intelligence and the Humanities," *Computers and the Humanities* 19, no. 2 (April 1, 1985): 117-22, <https://doi.org/10.1007/BF02259633>.

42 Nassim Nicholas Taleb, *Antifragile: Things That Gain from Disorder* (Random House, 2012).

# Backcasting the Way Forward: Actions and Implications



## **Think**

Create a Unified Vision for 6G Systems and Their Enablers  
Go Beyond DIME  
Enable Knowledge

## **Excel**

Understand Future Attack Vectors and Take Action

## **Fight**

Plan for Control in order to Enable Security

## **Pace**

Technological Determinism

## **Partner**

Build Relationships that Enable Resilience

## **Last**

Train to Enable Resilience Through Recovery  
Foster Adaptability

To develop responses to future threats, NATO uses a framework of “Outs.” These Outs are actions intended to out-compete adversaries. They describe aspects of strategic preparation and operational readiness to confront and defeat adversarial uses of 6G systems. The six Outs are Out-Think, Out-Excel, Out-Fight, Out-Pace, Out-Partner, and Out-Last. They frame the Threatcasting analysis and help to synthesize workshop participants’ visions for NATO actions, investments, and responses to future threats. Additionally, each of the six Outs has multiple subcategories that are consistently applied across each of the four findings. Some subcategories were more relevant to a particular finding than others. Additionally, the number of recommended actions does not imply importance or priority. Each alliance member will need to consider how best to implement these recommendations individually and collectively.

The broad actions outlined in the Outs below will have specific implications for NATO and other organizations. Following the guidance from the Outs, the below indications provide initial recommendations, which give NATO “a place to start” to design and implement solutions. This list is not meant to serve as a definitive collection of implications. It is, however, a foundation from which to build, add, explore and iterate.

## **OUT-THINK THE ADVERSARY**

How and what should NATO and alliance members do to out-think their adversary? How can they anticipate the adversary’s plans, create awareness of their actions prior to an attack, and make faster, more effective decisions once threats are revealed? To start, members must have correct information. NATO’s mutually-trained-intelligence-processes and personnel are critical for gathering and understanding the vast amounts of data, information, and intelligence needed to out-think the adversary. The Threatcasting data suggests mutually reinforcing activities, including developing a unified vision for 6G systems and applications, expanding 6G’s influence beyond the DIME model of national power, and creating a deliberate campaign of education both within NATO and to the general public. More proposed actions are outlined below.

### **Create a Unified Vision for 6G Systems and Their Enablers**

In the next decade, 6G systems will be developed and then deployed unevenly across the globe. Because the rollout will be uneven, NATO should develop a vision of access, employment, and implications for equitable use. In this vision, developers and operators must agree upon a definition of 6G systems and agree upon the technical and regulatory standards for these systems.

NATO must envision and govern the research, development, and use of the technology, including the human factors that come from 6G systems that are emerging online.

Commercial companies are already envisioning and designing the phones and devices that will use 6G broadband signals and other 6G connected systems. NATO may not have the capacity to strongly influence the commercial sector in what devices are built. Instead, NATO could be a world leader for understanding the implications of 6G systems on competition and crisis in the next decade. In particular, NATO should incorporate specific opportunities and challenges of 6G systems into such products as their next strategic foresight assessment and Future Operating Environment study.

### **Go Beyond DIME**

The future threat environment that will be enabled by 6G networks and the systems they support will create a range of new vulnerabilities and risks that because of their speed, scope, and scale cannot be dealt with by simply utilizing a DIME approach. DIME will still be necessary, but not sufficient enough to meet this challenge, because DIME often limits consideration to just the government's ability to employ national power.

To Out-Think the adversary, NATO must research, reimagine, and come to understand what is needed beyond DIME in order to disrupt, mitigate, and recover from the future threats of 6G systems. This includes the near certainty that 6G systems will be designed, employed, maintained, and regulated by private companies.

There are several alternatives that encompass additional elements of whole-of-nation power, including MIDLIFE,<sup>43</sup> PESTEL,<sup>44</sup> and DIME SEL.<sup>45</sup> These variations bring a number of factors into the framework, including legal and law enforcement, scientific and technical, political, social, or environmental. In the end, the acronym does not matter, as long as NATO takes a wholistic approach and considers all of a nation's power - not just its government's - when thinking about 6G systems and their effects on the alliance.

### **Enable Knowledge**

Because 6G systems are yet to exist, NATO must embark on a campaign to enable knowledge and information sharing that involves educating both the public and governments about the normal operations, expectations, limitations, and emerging uses of 6G systems. Specific proposed actions are outlined below.

### **Proposed Actions:**

- **Implement Robust Validation and Testing.**
  - o Validate and test all inputs to 6G systems with an emphasis on critical infrastructure controls and medical devices. This should include device testing in various bio-tech settings to ensure the compatibility, efficiency, and security of the devices across multiple platforms.
  - o Work to mandate penetration tests on FDA-approved medical and healthcare devices.
  - o Work to mandate penetration tests on 6G-connected critical infrastructure controls.

43 Craig W. Mastapeter, "The Instruments of National Power: Achieving the Strategic Advantage in a Changing World," Monterey, CA, Naval Postgraduate School (2008), <https://apps.dtic.mil/sti/citations/ADA493955>.

44 The Chartered Institute of Personnel and Development (CIPD), "PESTLE Analysis" (March 8, 2023), <https://www.cipd.org/uk/knowledge/factsheets/pestle-analysis-factsheet/>.

45 Konstantin Khomko, "A Nation Needs More than a DIME," *Defense.info* (April 3, 2019), <https://defense.info/williams-foundation/2019/04/a-nation-needs-more-than-a-dime/>.



- **Strengthen Data Security.**

- o Ensure there are security-by-design principles for 6G systems. This means encryption, data flow protections, and access rights. Root or admin parts of 6G systems must also be considered in the design phase of 6G devices and system components, not just added on at the end.
- o Develop and adopt strong data protection to prevent manipulation, including encrypted protections for citizens' personal identifiable information. Consider a pathway to incorporate future quantum-resistant encryption tools that can be added at a later date.
- o Implement a secure pipeline for accessing and transmitting training data to AI elements on edge devices to ensure valid models and guard against exploitation.

- **Develop Regulatory Measures.**

- o Through anticipatory exercises explore what agreements should be in place to deter misinformation, disinformation, and mal-information.
- o Regulate Deep Fakes and their removal as well as enforce a 6G bill of rights for data privacy.
- o Force transparency in bidding processes and social credit scoring data.

## **OUT-EXCEL THE ADVERSARY**

This section addresses how and what NATO and alliance members should do to out-excel the adversary. Questions answered include: How do they strive for excellence in development and detection? What research and investments should they make? What initiatives should they design? And what actions must occur across the spectrum from peace-to-crisis-to-conflict - both simultaneously and continuously? Achieving excellence depends, in part, on understanding the adversaries' motivations and capabilities; investing in the training, expertise, and tools necessary to counter potential threats; and developing shared infrastructure and capabilities to guide and regulate the evolution of these technologies. More proposed actions are outlined below.

### **Understand Future Attack Vectors and Take Action**

To Out-Excel adversaries, NATO will need to gain knowledge about the ways that they can hijack, manipulate, or spoof 6G systems. This includes ways that bad actors can disrupt 6G systems, specifically those that pertain to critical infrastructures that rely on 6G for operation. This activity will begin with members' intelligence communities (IC), but they will quickly need to expand to consider industry-wide information sharing and governmental oversight programs that are linked, but not part of the IC.

Once these attack vectors, vulnerabilities, and threats have been mapped and shared across member countries, investments and activities must be kicked off across the spectrum from peace to crisis to conflict. This will also need to include investment in new tools as well as processes and procedures.

## **Proposed Actions:**

### **• Implement AI Accountability and Security.**

- o Develop AI systems that can inspect other AI systems - essentially by “looking inside the black box”. Ensure these systems are also capable of monitoring IoT and medical devices for potential threats.
- o Foster greater transparency in AI system processes, alongside cyber defense systems for better security.
- o Launch a robust “bug bounty program” to incentivize strengthening the program.

### **• Improve Human and AI Synergy.**

- o Improve effectiveness of human decision-making when designing or responding to the advice of 6G systems.
- o Ensure that business leaders seek advisory guidance from a range of technology experts for informed decision-making.

### **• Diversify, Secure and Implement Advanced Supply chain Security Measures.**

- o Lessen reliance on a single type of technology, especially for critical sectors, such as food and technology production.
- o Require stress test systems that are responsible for these critical sectors, and conduct supply chain disruption tests for key components.
- o Develop and enforce stringent software and hardware validation processes. Updates should only be accepted from authenticated sources and rigorous checks should be performed.

### **• Establish a Global 6G Consortium.**

- o Build consortium with cybersecurity experts, technologists, and policy makers from various countries. The main objective would be to create and implement international standards, regulations and norms for 6G systems to ensure that its authenticity is maintained and potential risks are managed.

- o Collaborate with relevant regulatory bodies to enforce stringent cybersecurity requirements for all 6G systems.
- o Collaborate with human rights and international equality programs to ensure that 6G systems promote rather than minimize fairness and equal opportunities for access.

### **• Invest in Cybersecurity Research and Education.**

- o Encourage research on 6G systems and their vulnerabilities to stay ahead of potential threats.
- o Promote education and awareness about cybersecurity risks and best practices among NATO personnel and the public at large

### **• Enhance Data Consolidation and Analysis Capabilities.**

- o Use advanced analytics and AI to consolidate and scrutinize data from all use cases. This will help to detect anomalies and predict potential tampering or damage early within the design of distributed AI models.

### **• Build Redundant Safety Capabilities.**

- o Build redundant safety systems to avoid single points of failure and decentralize decision-making processes in order to prevent swift and potentially harmful actions.
- o Ensure multiple methods of communication with potential adversaries are in place. This will help in diffusing tensions and prevent escalation of conflicts.

### **• Promote Ethical AI Development and Use.**

- o Foster a culture of ethical AI use within the organization. This includes transparency in data use, continuous auditing for bias, and designing technology with the objective of reducing harm and promoting peace.

## OUT-FIGHT THE ADVERSARY

How does NATO out-fight the adversary? How does it deliver deterrence, defend the integrity of the alliance, enhance security outside its members, and ensure it maintains both a decisive military advantage and political cohesion? Combatting potential threats from 6G systems will require doctrinal, operational, and strategic changes to both deterrence and preparation for conflict. How should NATO expand-and-enhance its warfighting capabilities to meet adversaries who weaponize 6G systems? These questions are addressed in the recommendations provided below.

### Control Enables Security

To Out-Fight the adversary, NATO should explore the nature of control with 6G systems in place. The current concept of control is often considered as a technical mechanism with an assumption that there is a hierarchy of decision making that can activate the mechanism to increase or decrease the extent of security. In other words, decision makers at the top of hierarchies choose how much freedom or restriction is available to those lower in the hierarchy. However, 6G systems may be “flatter” than this. Developing centralized control will require a different way of looking at and approaching control within the 6G environment. The extent of security may range from minimal government involvement to partial regulation about technical aspects, such as spectrum availability and broadcast power.

This means that NATO will need to explore security without the ability of top-down control. This might take the form of security-by-design principles or processes to share data insights collected from IoT sensors with public and private partners. However, this also requires answering the question, “What are acceptable security levels for 6G systems?” The answer to this could rely on current and emergent cybersecurity best practices, largely agreed upon by the cybersecurity community. The answer could also come from the development of certain regulatory frameworks that then trickle down as a new or agreed upon standards that integrate with community standards.

During the competition phase, it’s recommended that NATO consider other elements of national power (e.g., DIME or other frameworks) in order to slow down global competitors from achieving parity in 6G system development. One example is for NATO to include economic programs that encourage NATO members to buy infrastructure and devices from other NATO members.

During conflict, NATO must consider how to technically disrupt, degrade, deny, or even destroy adversary nations’ 6G systems, while guarding against the same. This could include advanced research on electronic warfare applications, training, and doctrine that disrupt, degrade, or deny adversaries’ use of the RF spectrum. This may also require new concepts of electronic warfare and cyber confluence that affect AI applications on edge devices.

### Proposed Actions:

#### • Invest in Advanced Attribution Technology.

- o Develop or improve technologies to better identify and attribute non-human influencers and malicious foreign actors in cyber-attacks.
- o Improve misinformation detection and handling by implementing advanced algorithms to detect false information, coupled with swift reporting and investigation processes.
- o Develop and Implement Advanced Surveillance and Detection Systems. In the context of 6G systems, it’s essential to develop ways to detect, monitor, and handle potential threats posed by these devices.
- o In military applications of 6G, NATO should consider how “loud” friendly signal emissions are, so that allies are not giving away movements and positions from miles away. If emissions cannot be avoided, make them as secure as possible, and find ways to make them blend in with their surrounding RF environment. Make ally signals non-attributable, specifically to military activities.

- **Adopt Cyber Resilience and Deterrence Strategies.**

- o Build a robust cyber security team to disrupt, mitigate, and recover from threats.
- o Leverage 6G systems for deterrence below the threshold of nuclear deterrence. This might include dominance of adversary 6G systems through cyber and electronic warfare means or through economic pressure to reduce adversary acquisition and employment of these systems.

## **OUT-PACE THE ADVERSARY**

How can NATO and its members out-pace the adversary by using new policies, processes, and technology to minimize the risks of 6G systems and disrupt the adversary's decision-making process (OODA loop) in an 6G environment? This will not only require preemptive regulation and restrictions on 6G systems, but also the rethinking of logistics, communications, and planning in order to adapt in the face of new- and emerging threats. More proposed actions are outlined below.

### **Technological Determinism**

In the Threatcasting data, there were regular recommendations to create a new technological "thing" in response to an activity or action by a 6G system. This would mean that technology would be driving technology, rather than being led by human ideas. Humans should drive the development of technology for societal needs. A technology-centric mindset tends to lead to a problematic situation, such as an arms race, whereas a human-centric mindset seeks solutions and understands the implications of technology on people first.

Neither mindset is "better" than the other, but with advanced technologies like 6G systems, it is quite easy to be swept up in the excitement of the devices and "things" themselves and ignore humanity. On the other hand, taking a purely human-centric approach can delay technical development and/or provide solutions that cannot fully comprehend the outcome on humans. People tend to be creative creatures and adapt technology to their needs beyond the design specifications of that technology. Just because the technology promises something desirable, does not mean that the consequences can be known up front.

In 2022, NATO established the Defense Innovation Accelerator for the North Atlantic (DIANA) and a major endowment to fund research and innovative ideas. DIANA uses accelerator programs and releases "competitive call for proposals from deep tech innovators with dual-use application."<sup>46</sup> 6G systems are most certainly dual-use, and developers should be encouraged to apply for and collaborate with programs, such as DIANA, to improve 6G system resilience and security across military and civilian applications before adversaries develop counterproductive uses of the same technology.

### **Potential Actions:**

- **Promote STEM Education and Research.**

- o Encourage the study of Science, Technology, Engineering, and Mathematics (STEM) in educational institutions. This would ensure the development of a skilled workforce capable of building, maintaining, and innovating in 6G systems.
- o Build in technological "pauses" or rather, accelerate discussions on how advanced technology implications cannot be fully known at the outset. For example, consider the growing concerns on human-centric tasks and abilities that large language models exposed with the release of ChatGPT and similar applications in 2022.<sup>47</sup>

<sup>46</sup> Defence Innovation Accelerator and for the North Atlantic (DIANA), "About DIANA" (2023), <https://diana.nato.int/about-diana.html>.

<sup>47</sup> Bernard Marr, "A Short History Of ChatGPT: How We Got To Where We Are Today," *Forbes* (May 19, 2023), <https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today/>.



- **Implement Comprehensive Cybersecurity Measures.**

- o Conduct regular inspections of hardware and software.
- o Put in place security measures before the development and production begins. Developers should also integrate accepted best practices around network security rather than creating their own changes.
- o Ensure that security measures are regularly updated and that systems are maintained.
- o Prioritize investment in infrastructure, both physical and digital.

- **Build an AI-Powered Monitoring and Response System.**

- o Implement AI monitoring in devices and infrastructures to detect abnormal behavior and take appropriate steps in response. For instance, AI in cars can monitor route behavior and contact relevant authorities in case of abnormal activities.

- **Adopt a Human-in-the-Loop Approach.**

- o Implement human-in-the-loop authentication and authorization mechanisms to add an extra layer of security and decision-making in the use of technology. This can prevent unauthorized or malicious use of systems.

- **Promote International Cooperation.**

- o Advocate for international norms and standards for data privacy.
- o Establish agreements between NATO members to share information that can advance defenses and reveal vulnerabilities.
- o Form alliances that can share technical capabilities without entering into any political agreements.

## **OUT-PARTNER THE ADVERSARY**

How can NATO, its members, and affiliated organizations out-partner the adversary? How do they foster mutually beneficial, supportive, and habitual relationships with allied entities that can assist in such crucial areas as mitigation, deterrence, and recovery from threats? What exercises, organizations, and relationships are necessary to forge those links? And how should they expand those links beyond traditional nation-states and their militaries? These questions are addressed in the recommendations provided below.

### **Relationships that Enable Resilience**

To Out-Pace their adversaries, NATO will need to develop and maintain critical relationships that enable resilience. This would require developing and encouraging several types of partnerships, such as:

- NATO-to-NATO country partnerships, which include bilateral agreements and full alliance collaboration.
- Government partnerships with public and private entities that are not part of the military power infrastructure.
- Private-to-Private relationships, which may include NGOs or other bodies that are not government controlled.

### **Proposed Actions:**

- **Forge Partnerships with Underserved Countries and Areas.**

- o Collaborate with lesser developed nations and communities to share knowledge, technology, and resources. This could help to create a more balanced and inclusive global technological landscape. It would also help emerging nations to be more resilient against the misinformation, economic advances, and diplomatic pressures of NATO's adversaries.

- **Promote Cross-Cultural Knowledge Exchange.**

- o Encourage cooperation and collaboration across nations and sectors to combine cross-cultural knowledge. This is expected to lead to more innovative solutions and a broader perspective on global challenges.

- **Strengthen Western-Originated Industry Players.**

- o Improve the competitive edge of Western technology companies by providing them with necessary resources, access to innovation, and an enabling regulatory environment. The DIANA initiative is one way to ensure NATO members have sufficient funding for research and innovation.
- o Create unified international laws on data privacy to safeguard individuals' data rights.

- **Improve Data Sharing and Analysis.**

- o Share records and anomalous errors across organizations to improve data analysis and identify significant trends.
- o Encourage collaboration and information sharing between different agencies and sectors to tackle shared challenges.

- **Educate and Empower the Next Generation.**

- o Develop programs to educate young people about technology use and misinformation. Equip them with skills to sift through false information and use technology responsibly.

- **Enhance Public-Private Partnerships.**

- o Collaborate more closely with the private sector to leverage their capabilities, improve system security, and maintain state-of-the-art technology. This could involve sharing development capabilities and fostering tech alliances without political agreements as well as leveraging private companies for maintaining system security.

## **OUT-LAST THE ADVERSARY**

How does NATO, its members, and their societies out-last the adversary? How do they achieve and maintain a long-term perspective on potential threats and cultivate a culture of resiliency in response? These two questions are addressed with the following recommended steps.

### **Train to Enable Resilience Through Recovery**

To Out-Last the adversary, NATO and members will need to train for these future threats via exercises, planning, and/or other activities to make the 6G system safer. These exercises and events must consider the role that private companies and even individuals have in the development and use of 6G systems. 6G systems are expected to fail, so practice warfighting under degraded conditions and with analog backups until the system can be repaired.

### **Foster Adaptability**

Adaptability is normally a "human" endeavor, but occasionally also indicates automated fail-safes as long as they are programmed to take advantage of security-by-design principles. For instance, automated weapon systems without a human in the loop (of which there are currently very few) would need to demonstrate human-level adaptability in new and untrained situations to be trusted enough to continue to not need human intervention. If adaptability is not proven, then the decision to shoot would necessarily fall back on a human. With that, more recommended actions include:

- **Develop and implement programs and structures to help NATO member states and their citizens to recover from and adapt to 6G system threats.**
- **Develop and implement backups, analog systems, fail safes, or human-in-the-loop decision making to increase adaptability.**

- **Invest and Improve Social Welfare.**

- o Implement strategies to address poverty and facilitate better integration into society. Provide support for those experiencing social isolation, especially after significant emotional events.
- o Provide access to national healthcare and invest in workforce training and education.

- **Prioritize Long-Term Strategies.**

- o Focus on strategies that prioritize longevity over immediate gains. This includes building in upgradeability into systems to ensure they can evolve to meet future challenges.
- o Maintain a long-term perspective by keeping humans in the loop in processes, such as manufacturing, healthcare, and critical infrastructure - rather than solely relying on autonomous technologies.

- **Enhance Information Sharing.**

- o Create a culture of open and efficient information sharing across NATO and its members to reduce unnecessary silos. This could involve setting up regular exercises to detect unusual behaviors or malfunctions as well as having multiple organizations and members share analysis and auditing results for diverse perspectives.

- **Implement Threat Intelligence and Resilience Strategies.**

- o Maintain vigilance on potential adversaries and their activities
- o Emphasize resilient systems with limited complexity.
- o Develop countermeasures and backup systems to ensure recovery from attacks.

- **Promote Transparency and Oversight.**

- o Encourage transparency of data access and sharing.
- o Implement financial regulations and oversight of 6G systems and their associated businesses, while providing the general public evidence of regular security scans and updates.
- o Educate individuals from a young age on values, initiative, and autonomy.
- o Train officers, soldiers, and the wider public on the implications of technology advancements like 6G systems on society and security.

## Conclusion

The advent of 6G technology presents both remarkable opportunities and potential threats. Envisioned in science fiction for decades, the arrival of this hyper-connected reality is inevitable and nuanced, intertwining both positive and negative aspects. With paradoxical co-existence of utopian and dystopian attributes, this 6G world may be fueled by the startling readiness of humans to forfeit privacy for the sake of progress. 6G may be a catalyst for a world where connectivity is a double-edged sword, driving progress, while potentially isolating members of society further, compromising privacy, and increasing vulnerability. It is essential to discuss these challenges and opportunities that humanity may inadvertently forfeit in pursuit of technological advancement.

For NATO and militaries, 6G systems further redefine the modern battlefield as an increasingly global, heavily populated space that is driven by technological advancements, which make every connected entity a potential target. Civilian technologies integrated into this modern warfare landscape further complicate the intricacies of identifying “friend from foe,” especially within the information environment. Moreover, the physics-based challenges of 6G will likely require ubiquitous towers and connection points that subsequently provide an unmanageable number of access and attack vectors.

Ultimately, these challenges have the ability to foster a hyper-polar world and a shift of power dynamics in which nation states, activists, and terrorists all have the same access opportunities for nefarious activity. These attack vectors are likely to be intertwined with privately controlled and operated infrastructures. This dynamic creates a challenge in control over 6G technologies because it is likely to be beyond the reach of a single entity. Therefore, to secure critical infrastructures in a 6G roll-out, what’s needed is a global consortium of public, private, and governmental partners.

Finally, as 6G systems are implemented, a host of new tactics and hazards emerge, such as ‘Six-jacking’. Primed by society’s over-reliance on data collection are also risks to nation stability - due to potential exploitation of 6G systems. Covert manipulation of these systems complicate society’s ability to discern nominal and abnormal performance, and fundamentally shorten response times. Therefore, while companies and nations race towards this hyper-connected future, understanding and managing data and its connections are perhaps the greatest challenges to face. A wholistic, global effort is required to navigate these complexities, ensuring that the advent of 6G technology fosters a future of progress, security, and prosperity.



## Appendix A - SME Transcripts

### **SPEAKER A - DR. RICHARD WITTSTRUCK | SENIOR INTELLIGENCE ADVISOR, USA**

*Thu, Feb 09, 2023*

#### *Summary*

6G technology is projected to introduce unique challenges and opportunities for military forces, both allied (Blue Force) and adversarial (Red Force). For the Blue Force, 6G's higher frequencies of operation, faster speeds, and lower latencies enable more efficient command-and-control communication, with large bandwidth products and services accessible in real-time. This technology facilitates the rapid distribution of command intent and intelligence products throughout the entire force structure. However, the advent of 6G also presents challenges from a defensive perspective. Our current sensing technology will need to evolve to detect the higher frequency terahertz emissions from 6G nodes. Investment strategies from now until 2040 need to focus on how to detect, intercept, and accurately locate these emissions.

Additionally, the application of 6G to fire control mechanisms could enable real-time weapons delivery, thus posing significant challenges for the allied forces. This swift communication could pave the way for AI-driven fire control mechanisms, replacing human intervention and speeding up target acquisition and weapon deployment. For both allies and adversaries, 6G can transform the battlefield, increasing the need for advanced sensing capabilities and cyber defenses to protect against counter-6G technologies. We must also prepare for the use of 6G in cyber and information operations, where rapid dissemination of misinformation or disinformation can occur. In summary, while 6G can be an enabler in many domains, it also demands significant adjustments in our technical development, operational strategies, and information management to counter potential threats.

#### **SUMMARY KEYWORDS**

ability, allies, capabilities, challenge, command, commanders, control, domain, echelon, emitters, enable, fire, higher frequencies, investment strategy, network, nodes, operations, order, present, technology

#### **TRANSCRIPT OF RECORDING**

"I am Dr. Richard Wittstruck. I am a senior intelligence adviser to the United States Army Assistant Secretary for Acquisition, Logistics, and Technology. In that position, I look very closely at advancing technologies and the impact they may have on the battlespace into the future. For the United States Army, that means two time horizons today. One is 2031, when we expect to be able to deliver a ready, sustainable, and modernized force against the latest threats, and 2040, when we look to deliver a fully, multi-domain-operating force, which can operate not just the geospatial, and spectral means, but also in logical and cognitive environments.

So, with that as a framework, we want to talk a little bit with you this morning about 6G - and why 6G? Because 6G presents new challenges in the battle space for both the Blue Force and the Red Force, allies, and enemy, if you will, respectively. And the problem that we see forthcoming or the challenge that we see is both an opportunity and a challenge. For the Blue Force Commander, with the advent of 6G technology that provides us higher frequencies of operation, higher speeds, and lower latencies, we can see very readily from a command-and-control perspective and a communications perspective at every echelon, a prolific nature to 6Gs ability to cascade across the battlespace, providing ubiquitous access to every echelon, to large capacity and large bandwidth products and services that heretofore they have not been able to access in near real time, if not real time.

So, this will provide the Blue Force Commander an enabling tool to be able to use the lowest tactical echelon to get command intent out, to get large products - like intelligence products, data products, and the such - out over the enterprise and into the hands of commanders at all echelons with a common understanding of intent, and timing of operations.

With that said, if we turn the reticle around from an opposing force commander's perspective, the challenge that this technology may enable is the fact that we will now have to step back and rethink our sensing investment strategy on how we will be able to sense these emitters on the battle space to form an electronic order of battle and associate that electronic order of battle with organizational orders of battle. Because now that we're going to higher frequencies, we are going to see some distinct cutoffs in our current sensing technology's ability to collect those frequency emitters. So, we are going to have to look at an investment strategy from now through 2040. Now starts to get up to those higher frequencies of how we detect, how we intercept, how we direction find, and how we precision locate terahertz emissions coming off of 6G individual nodes as well as enterprise-hub nodes.

With that said, if we are able to accomplish that, and we are able to establish a true electronic order of battle associated with an organizational order of battle, our next challenges will be to deal with the enemy's C2 network, which may be employing 6G in much the same way I have described our Blue Force commanders being able to use it.

So, they too will have prolific dissemination of command intent, of orders of command and control, and the such, in a high-speed, low-latency environment. Which will make it difficult, now, to determine from a low probability of intercept/ low probability of detect perspective, where they are in the battle space, because this low-latency of 6G enables them to have burst communications heretofore, one hundred-times faster than what we see today with 5G.

So, therefore, it is going to be a very short on-time for those emitters to be found, and for those emitters to understand exactly the command-and-control construct that's being employed amongst emitters and hub nodes in the battlespace.

The other challenge one can see, is when one looks at the fire control mechanism on the battlespace. An implementation of 6G is part of a PACE plan - Primary, Alternate, Contingency, and Emergency plan - of fire control. We could see 6G integrating into that PACE plan for the purposes of providing a new time definition to time critical, if not time sensitive targeting. Because, with that latency greatly improved 100 times over 5x, excuse me 5G, we could be looking at the advent of real-time weapons delivery, based on command-and-control issuing of orders. So, there won't be a latency time to go from command to firing an effect, and that could prevent present new capabilities and capacity challenges for allied forces, as we try to determine - how we are going to cover-down on a battery of 6G-enabled fire control assets and armaments that may put us in a position where they can volley more capability at us, in terms of ordinance, in a much shorter time, simply because the fire control mechanism is that much more rapid.

And it isn't just the rapidity of the fire control mechanism that now creates both an opportunity and a challenge. But what it allows now, is to take man out-of-the-loop and really go into a full engagement of artificial intelligence - machine learned - fire control mechanisms, by which, we'll see the traditional human intervention of weapon target pairing, as well as seeing targeteering calculations replaced by computer-driven algorithms, that operate on a very robust network enterprise, that allows for the ability to actually capture tactical, operational, and strategic target sets in near-real-time, and then prosecute them in record time.

So, when one brings together all of these things, 6G presents to the battlespace both a Blue Force enabler, but also a Red Force enabler that will create new challenges in a multi-domain battlespace for the Blue Force Commander moving forward into the future.

So, if one were to look into the crystal ball today, and talk a little bit about where those investment strategies would be - well, I have already discussed new sensing capabilities that will be required in order to get to the higher frequencies - the terahertz frequencies - of operation of 6G. New processing, exploitation, and dissemination algorithms and capabilities may have to be developed in order to understand those collections, and translate them into meaningful information and data for use by the intelligence community, by the command-and-control community, and by the fire's community, to effectively plan maneuver and effects operations across the battlespace.

In addition, we are going to have to start looking at - how do we prevent and protect our 6G from counter-6G technologies that any future adversary or enemy may want to employ to either spoof our network and/or jam our network to degrade, disrupt, or deny our ability to take advantage of those 6G speed latency and capacity issues?

So, with that said, one now has to start to begin to unpeel, if you will, from that onion, the different layers of technical development that's required in scope, but also in time. So, as I said earlier for the United States Army, that means that we'll be looking at - how do we target evolution in 2030, when 6G is forecast to show up, as a new emerging technology potentially on the battlespace? And then, how do we prepare for that emerging technology throughout the 2030s, as we approach 2040, and are we now going to be operating in a fully enabled multi-domain operation?

So, if I pull MDO apart, just for a moment. So, we're looking at the fact that in the geospatial sense, we could be seeing many more emitters prolific across the battlespace, performing multiple warfighter functions simultaneously, in a large capacity way, and we would have to sort through that and make sense of that very quickly, not just in location, but in intent.

Then, we would have to look beyond that into command-and-control and make a determination on an operational order of battle - exactly who is the command-and-control node amongst that enterprise of prolific emitters? And how are we going to set criteria to understand what a command-and-control node looks like in such a network, because of its ability to have short on-communications and rapid communications?

Again, low-probability-of-intercept, low-probability-of-detect, and the ability to characterize a voluminous command-and-control node versus maybe a down trace receiving node that's taking orders on one particular part of the mission. And then lastly, on fire control - how do we speed up the clock, if you will, on conducting fire control missions, such that we can keep pace and operational tempo with the enemy, as they're presenting multiple threats, at multiple times, in multiple parts of the battlespace using a very robust 6G network, which is going to allow them that near-real-time sensitive and critical targeting capability?

So, when you bring all of these things together, it starts to expand into a multi-domain operation that transcends, not just geospatial and timing, but also frequency or spectrum. And then, if we turn to the logical domain in cyber, the concept of a cyber network operating in 6G would also present, again, both opportunities and challenges to allies and commanders as we try to determine - how does one protect against a multi-pronged attack on cyber via 6G, which may be done in such a rapid sense of milliseconds, that we may not have time to respond unless we have the appropriate AI/ML capabilities to do so?

And then lastly, as we turn to the cognitive environment, more specifically, Information Operations, and we see 6G take over the world, in terms of its ability to displace 5G and precedent commercial Internet standard, in terms of doing social media, for example, in broadcast media - how does one entertain Information Operations in a 6G environment where now I may be presented with multiple dilemmas in social media? -And we'll have to sort through those very quickly to determine what is real, and what is a deep fake, simply because the 6G network will enable that many more social media nodes to be presented to the world with stories that may be filled with misinformation or disinformation. And somehow, we as allies, are going to have to sort through that and get our message out, strategically, on what the truth is of what's going on in the battlespace and around the region of the battlespace, so that those individuals and host nation populations that are involved in such conflict, can truly understand what's going on and dismiss most of the disinformation/misinformation.

So again, 6G, in its final state looks to be an enabler in all those domains of geospatial, spectral, cyber, and cognitive. So, if we take that as our future operating environment, we have to begin now to start laying groundwork on the science and technology development, leading to material development, coupled with combat development - specifically, concept of operations and tactics, techniques, and procedures - that we will have to present in order to create dilemmas for the enemy, while deflecting any dilemmas that they try to present on us via 6G.

So, I think in closing, what I would say to you is, 6G is not something new, in terms of our ability to provide our combined arms an ethos of looking at a new threat, as both an opportunity for our employment, and a challenge in the event that adversaries and enemies employ it against us. I think if we can stick to our doctrine of combined arms, as both nations and as allies, we can work our way through 6G, but with an understanding that the timing clock gets faster, the capacity is faster, so the throughput is faster. And as such, we're going to see this present itself in both advantageous and disadvantageous environments as we look to the future in an attempt to figure out - how does one win a multi-domain-operations environment?

So, in closing, thank you for your time, and I hope this has been helpful to you to make sense of 6G."



## **SPEAKER B - BOB HARRISON | POLICE, RAND**

Mon, Mar 20, 2023

### *Summary*

6G is associated with edge computing and is predicted to revolutionize various sectors, including law enforcement. Artificial Intelligence (AI), like ChatGPT, is playing a crucial role in this, offering efficient, user-friendly capabilities, like consolidating diverse inputs into a single document for police reports, and providing real-time information. These benefits are counterbalanced by the need for effective system management, the potential for misuse, and the necessity of deploying technology responsibly. There are ongoing debates about the implications of AI on the arts and social dynamics, exemplified by DALL-E and micro-investing in Africa. Edge AI, becoming feasible with the transition from 5G to 6G, allows individuals to manipulate and rely on information more effectively, potentially leading to increased isolation in our increasingly connected world. Concerns arise as people retreat into artificial worlds, potentially straining social fabric and exacerbating political and cultural divides.

As we embrace 6G, we are moving towards a network of intelligence, characterized by low latency and higher bandwidth. The technology is also a promising tool for mitigating numerous traffic-related fatalities. However, the interconnected nature of these systems brings about vulnerabilities, such as susceptibility to hacking and misuse of personal information. With network slicing and sharing, users will be able to curate their realities, possibly leading to increased tribalism and isolation. This can also affect governance, as the digital space can allow for widespread communication, but potentially less sincere dialogue. As AI and 6G evolve, the future could resemble either the *WALL-E* or *The Incredibles* narrative, depending on how technology is utilized. In one scenario, technology could isolate and displace humanity, while in the other, it could act as a companion, elevating our capabilities and strengthening communities. These contrasting possibilities underline the importance of responsible technology deployment, as well as the necessity of creating equitable access to future technological advances.

## **SUMMARY KEYWORDS**

AI, create, emerging, fact, future, generations, *Incredibles*, intelligence, intensified, network, opportunity, people, policing, public safety, software, technology, threat, ways, world

## **TRANSCRIPT OF RECORDING**

"6G is edge computing. The one of the aspects that is related to edge computing is the emergence and now in the public's consciousness, ChatGPT and its kindred across various platforms, where we're seeing actual user friendly, interoperable artificial intelligence that in many ways could present great opportunity. We're looking at it in policing as to whether AI can help officers complete excellent police reports they don't have to write. Where they have body camera footage, they have a lot of different inputs that can be consolidated into a single document for prosecution or to record the essence of a crime that doesn't take an officer out in the field for hours at a time. So, there are some phenomenal capabilities that even now we're starting to explore in building penetration, ubiquitous software intelligence, to give officers real-time video, real-time tips, and real-time information in a crowdsource fashion from communities, as they experience threats to public safety. Difficulty with that being managing systems, developing them forward, and then being able to use them, as intended, while not either inadvertently or intentionally misusing them.

So, as we look at 6G, and I think the ChatGPT is serendipitous because we see some of the same things, I am more of an optimist. I think that technology, no matter what technology we're talking about, is neutral. It's the manner in which it's deployed, who by, and for what purpose that gives us the effective/ineffective, or for lack of better words, the good and the bad. You know, we can optimize without nuclear energy, certainly wouldn't have the fantastic tragic capacity to destroy things. We also wouldn't have nuclear medicine and cures to cancer. So, we start thinking about technology as a platform or tool, and that there needs to be human constraints and technological constraints on its use to optimize it without also opening threats that can be exploited by small groups of dedicated people who have high levels of knowledge and low levels of constraint.

So, you do have with AI right now with DALL-E and the art world; there's a fantastic debate going on as to whether or not that's really art - where you can input you know: paint me or Ferrari, as Monet would have done, and something comes out the other end that's actually pretty remarkable. Or, show me: a dog sitting in a field of flowers, as Pissaro might have presented it, and it comes out looking very, very similar to something, had they had seen that context, would have been that way.

It then again offers fantastic opportunities. You look at micro-investing in Africa, in Sub-Saharan Africa. You look at what the Air Force's Blue Horizons project, more than a decade ago, talked about super empowered individuals. As you move to edge AI, which is starting to become possible with the software- defined networking of 5G moving into 6G, you really have people that can access manipulate information, rely on their AI to do things with and for them to be connected. Now, of course, we've already seen, as a connected world, doesn't mean we are closer. In fact, we've become more isolated.

I think the social isolation - not only artificial intelligence, virtual reality - the isolation we have to retreat to online platforms and see those that are our friends and community, rather than people who live with us are threats today, and I think will intensify as technology becomes more attractive, easier to use, and produce better results. So, I see a social fabric issue, which we see politically; we see culturally; we see with gender identity; we see in many other ways, can actually be intensified adversely by virtue of having access to an artificial world to which one can retreat, and very rarely has to come out of. So, there are great opportunities.

There are also potential threats. I think, from a police world, and understand as a cop, that the police tend to view the world as one big felony in progress. They kind of see a threat in everything, which is pretty much their job. You know, we would hope that with the normal people out there, and most of the people we talk to, that you don't see life in that fashion because you don't have to.

That is the police become more adept at mitigating threat, as they can recognize why networks have gaps in security, the opportunities that multi-access edge computing can possibly offer, and how spectrum sharing is something that can be done for the good rather than looking at everybody as a potential Blackhat.

So, as we think about 6G, one of the significant moves forward that we'll see is we're going to move from an Internet-of-Things to a network of intelligence. You'll also have a much lower latency. As the bandwidth increases, you'll have near zero latency, which is a requirement for useful, ubiquitous autonomous vehicles. One of the goals of the federal government is to reduce, if not eliminate, the 30 to 35,000 people who die every year in traffic collisions. Those right now and we can see, you know, certain cars catch on fire, or certain cars that have crashed when in self-drive mode, people were very fearful of - oh my god, if the cars drive themselves, they'll just crash everywhere. Which, I would challenge them to think of any car that could be less safe than a 16-year-old or 85-year-old might be driving it, you know, that it will, in fact, allow us to drive more effectively and efficiently. Allow traffic jams, hideous traffic jams to cease to exist, because the flow of traffic can be moderated much more effectively, to enhance the safety to the point that we actually save lives.

Now, of course, the threat being, and we've already seen documentary footage, that people can hack into interactive electronic systems and manipulate what they do. And I think that, to me, probably the greatest vulnerability in 6G from a threat perspective, is its susceptibility to not necessarily even over hacking to perhaps, you know, rig a nuclear reactor to go offline and create a disaster, or to stop all traffic for a purpose, is the nominal ways that software can be coded, and utilized to gather intelligence information, to scrape data, to glean personal information, to essentially, you know, rig outcomes that are very, very difficult to find because of the complexity of the network itself.

So, we can look, perhaps in, Apple's App Store where there are literally hundreds to thousands of apps available. When we look at user data on a smartphone, most users use fewer than seven of the apps. And I think that'll be intensified, as we look at network slicing, we look at network sharing; as we look at this super-connected- individuals, that people will be able to define and curate their reality in ways that match their emotional, psychological, and intellectual needs, and start to exclude others. You have the tribes, you know, this is my tribe that is technological. It aligns with these apps, these worldviews to the exclusion of others. And I think politically, we've already started to see that where it used to be whichever side of the aisle you might be on, you would think that: well, those are good people, bad ideas.

And in fact, it's much more normal to think: well, those are just bad people. And I think as we move online, remote electronic, that, in and of itself, becomes intensified. There's a lot of emerging understanding of the isolation, the lack of marriage, the lack of relationship, that perhaps, you know, social media, and dating apps themselves may intensify behaviors that isolate people from one another, and actually inhibit relationship development. And not just necessarily for intimate partners, or for a dating app itself, but as we start thinking about the fact that America, in many ways, was founded on the town hall. We would gather together; there was direct democracy; people would be heard on any side of an issue and talk about any aspect of a problem that they themselves are experiencing in the group itself. The community itself, would decide the best path forward. And we talk about electronic town halls, we look at EV, in fact, we look at the medium we're in now, we can reach far more people, but have far less sincere dialogue. And as we have moved to a representative democracy in this American republic, it's, as Winston Churchill said - it's the worst form of government ever invented, except for all the others - that I feel this breakdown in governance, which can be intensified by isolating oneself online is one of the threats that over the next decade, I think we'll continue to see.

I think that as 6G helps us; as AI helps us; we also face the same opportunity to be much more effective in a narrow band, and much less connected across bands themselves. Even as you sit at wraps on autonomous platoon of 2000, 3000 cars traversing the San Diego freeway in Los Angeles - you're totally alone.

We have one of two futures ahead, and these are extremes, but perhaps is a thought bubble - something to consider. And those would be the difference between what I would term a *WALL-E* future, for those that saw this movie years ago, of humanity that had become the masters of a fairly sophisticated fleet of robots to do their bidding. But in that fashion, never left their chairs, became incapable of doing anything for themselves, as the world was brought to them - food, entertainment, devices - to the point that in this environment, that people sitting in the lounge chairs will be transported to another place to experience something else, but never actually have to get up, move around or interact with people that weren't already around them.

You also have been as opposed to *WALL-E*, to stay within Disney entertainment, perhaps *The Incredibles* future. If you remember *The Incredibles*, they were a kind of a normal suburban family, but endowed with superpowers. They used the superpowers because of the technology to do wonderful things, to become closer as a family; to create not only a stronger family structure, but a safer community. So, it does depend on how people use 6G - how they use artificial intelligence, how they use virtual reality - all of which can come together in a very useful or very threatening way. Will they want to experience more of what we see now, a *WALL-E* future where - obesity in America has become an epidemic; where people are fractious and fractured; where they lob bombs from their couches on the internet through reader responses - and can in fact, Doxs, Hex, Bex, and destroy opponents without ever leaving the comfort of their home. So, that's looking at technology being used in passive and unsought ways that displaces humanity.

Or, in the *Incredibles* future, are we going to use technology, I think as those who create it envision it? It's a companion, not necessarily a servant, but a companion itself, to: intensify and elevate our capabilities; to allow us to reach further; to allow us to help others; and to allow us to actually create community and create stronger relationships with those with whom we are in contact because we have technologies to actually help. The - you don't stand by saying: "oh my god, someone should do something," but I have the ability to do something. So, those are kind of the two and metaphoric futures, that I think in all seriousness, we do face.

So, as we move out 10 years and we look at this disaggregation and virtualization of data; as we look at this hyper connection; as we look at inevitably the disruptive technologies that will emerge if someone sees the capability, someone else is going to say "Oh, I could use that for this" - the old what-if future used either unproductive or non-productive generations. And then, how do we manage energy? How do we manage battery space? How do we actually connect? And in many ways, how do we effectively coexist with an increasingly sophisticated artificial intelligence; that I think has long been in science fiction; that in our lifetimes, can become science reality. That it is science-fact that you have, perhaps a silicon-based - what we would now call a robot or Android - who can act and interact in very seamless ways; can communicate with us effectively, in either virtual space or in meet-space; can help us be what we can be; protect us from what threatens us; and then be there for and with us, as we are with them.

So, look for this *Incredibles* future, that I think we can actually optimize and survive some of the ridiculousness that we see nowadays. If, in fact, we allow the technology to manage us; if we use it as a shortcut to never have to leave our home; to perhaps watch exercise, but not engage in it; to see events, but not participate in them; and to meet new people; to experience the world; to meet different cultures; eat different foods; and listen to different worldviews; I think that, to me, is the greatest threat, as we are becoming super empowered individuals.

So, to me, you always want to think (and as I talked to groups about the future), recognize a few things. And one of the most important ones is that if you don't have a seat at the table, you might be on the menu. And it's not to protect what is against what may be, it's to move from where we are to where we can be, for the productive use of society in general - all the way from the larger national and international framework down to the individual and the people they know. So, that kind of concludes my thought about 6G. I think it's very, very ragged. As William Gibson, a science fiction author, once said: "The future is already here, just not evenly distributed." How do we distribute it in a way that is equitable? How do we optimize and leverage the technologies and the intelligences that are becoming possible in ways that are productive, and that also cauterize off those who might intrude; those who would use it for either financial or political gain to work against us?

So, that concludes my time. Thanks for listening. I really appreciate the opportunity to learn more from the work you do and to see the final product. Thank you."



## **SPEAKER C - DR. TIM PERSONS | TECHNOLOGIST**

*Wed, Feb 22, 2023*

### *Summary*

6G technology, expected to emerge in the mid-2030s, is anticipated to provide presence-like experiences, transforming our current understanding of telepresence. The predicted capabilities of 6G, including drastically reduced latency, enhanced computing power, and significantly increased data rates (potentially up to a terabit per second) enable the convergence of technologies that create a feeling of being truly present. This improvement from current telepresence practices could potentially revolutionize sectors like warfare, making it possible for soldiers to remotely control drones - with the same sensory awareness as being physically present. However, this advancement also carries a dystopian potential - with amplified edge computing, we are essentially positioning AI everywhere. This brings with it, the risk of advanced hacking or data poisoning of AI systems that could lead to a loss of control over devices, jeopardizing battlefield dominance and situational awareness.

The second key element of 6G technology is related to the data it will handle. The amount and speed of data circulating will redefine our concept of storage, potentially creating next-gen cloud systems. Another significant aspect is its capability for full-location awareness in all four dimensions (three-dimensional Cartesian system plus time), potentially offering super-precise location tracking. While this could provide unprecedented opportunities for intelligence collection and information dominance, it also poses significant risks to privacy. With the aid of 6G-enabled AI, everything and everyone could be tracked at all times, leading to a state of Orwellian omniscience. As such, while 6G technology presents promising opportunities, it also demands careful consideration and risk management, especially in the national security sector, to protect individuals and maintain their ability to thrive in the future.

## **SUMMARY KEYWORDS**

AI, amplified, apparatus, compute, data, dominance, drive, edge, enable, future, imagine, moving, narrative, rates, talking, technology, telepresence, terabit, terms

## **TRANSCRIPT OF RECORDING**

"Hi, my name is Tim Persons, and it's a pleasure to be part of this activity. I am the former chief scientist of the U.S. Government Accountability Office, where I served across the entire enterprise on science and tech issues, including 5G and IoT, AI, and machine learning, and so on. But, I also served as its managing director for the whole science and technology team. So, it's a pleasure to be here and be part of this Threatcasting workshop.

When I think of 6G; when we think about the mid 2030s, and timeframes, I think that really there are two key things that come to mind. One is the idea about true presence-like technology. So, you may be familiar with telepresence - and that's something that we've all become quite familiar with, especially as we've gotten higher bandwidths and higher data rates and things like that, that we've all experienced by working remotely through the COVID-19 pandemic. But, this with 6G, when you're talking about moving 2000 times the performance of 5G networks in terms of minimizing latency, the power of computing behind it, and the massive amounts of data that are going to come with potential peak data rates - which are still not known, but imagine data rates of a terabit per second, in comparison to 20 gigabytes per second. So, that's sort of the, the scale that we're talking about. But, it really, I believe, allows you to imagine a presence-like convergence of technologies, where you are there. That means a little less than kind of the Sci-Fi avatar movies, but more than what we are doing on our screens and things today, and calling it telepresence.

I think that has profound implications for the future of warfare. When we think about drone technology and people working in joysticks, what if you imagine a presence technology, enabled by 6G, that places you in the apparatus, in the moment, and you have full sensory awareness, as if you were there.

-And I think that for close-combat, urban warfare environments; I think that's very powerful, indeed. Now, the dystopian narrative with that is because when you think about 6G, you're thinking about really, if we have been pushed to edge computing, powered by 5G - in other words, we're moving from compute from the core into the edge. In 6G, what you really are doing is amplifying even that compute at the edge, where you're really talking about AI at-the-edge.

And so, AI with a presence technology framework and a human-enabled by AI or various tasks and so on, has a dystopian narrative. If you can data poison the AI, you can hijack the computer-at-the-edge, it's like an advanced hacking type contest that if you lose, you lose control of your apparatus; you lose control of battlefield dominance, situational awareness, and so on.

So, there are key things that are both and always with technologies; you're going to have a double-edged sword narrative on that. But again, an exciting future where AI is now pushed-out from a core high-compute paradigm into the edge. And that means AI everywhere, which means risk everywhere, as well as opportunity everywhere. Data is just going to be going around and at such a voluminous rate. I can't even imagine a thing where optical-like, I'll put "storage" in air quotes, in the future is the thing where the bits are swirling around there and what it's sort of the next-gen cloud. And what that would look like to have data that's, that's stored in that way, and yet still can move at the speed-of-light and be driven by 6G - that's a very powerful, and yet scary thing.

The other thing I think, is, when you're talking about that much data, it's a full location awareness in all four dimensions, right? So, in the Cartesian system plus time, you're talking about knowing where things are.

I think about our GPS systems today, and they're very good at doing you know, sort of a 2D mapping, it helps us drive our cars around - that's very cool. And I think that when you're talking about 6G, it's going to have super-precise location in three dimensions, and as you're being tracked - because we're talking about full situational awareness by the network, by the system - then, it can track you everywhere you go. There won't be any concept of what we think about in terms of privacy today. And so that, that lays the groundwork for an incredible opportunity for intelligence collection, and things like that - military dominance, information dominance. At the same time, if we are in that space, it means that everything can be known.

So, we will remember that we had a forward operating base that was discovered just by some Fitbit-type software that was tracking where all things were going. Imagine that, amplified by 1000s of times in terms of its precision, its duration, its knowledge of everything where everything/ everyone is going, and then when you enable AI, as 6G will enable in that case, you can have an Orwellian omniscience about everything going on, on a given location.

So, very exciting time, and yet something that of course we need to think about in terms of caution. So again, presence-technology, location awareness - all based upon the convergence of these technologies. Compute and AI moves out to the edge, and that's going to drive a lot of the risk management that we're going to have to face in the national security sense to protect our warfighters, and yet, still enable them to succeed in the 2030s and beyond. Thank you."

## **SPEAKER D - DR. TOM RONDEAU | OUSD(R&E)**

*Thu, Mar 30, 2023*

### *Summary*

The future world of 2035 will be dominated by the sixth-generation mobile system for wireless communications, or 6G, as depicted by influential dystopian novels like William Gibson's *Neuromancer* and George Orwell's *1984*. While these novels warn us of potential hazards, they also illuminate how technology, particularly 6G, might impact people, societies, and cultures. 6G promises to offer several innovative capabilities, including native AI/ML, enhanced energy efficiency, and extended reality (AR/XR) services, resulting from ultra-low latency and universal coverage. Other features include seamless global connectivity through terrestrial deployments and non-terrestrial networks, integrated sensing and networking for contextual solutions, and hyper-localization services, enhancing our engagement with the cyber-physical world. Using these capabilities, we could witness a future with improved AR/XR devices, perfectly orchestrated supply chains, remote medicine, zero-touch provisioning, intelligent agents, collaborative robotics, and autonomous network vehicles.

However, the implications of 6G technology also entail challenges and risks. Cybersecurity risks, novel attack surfaces due to improved localization technologies, and the potential for ubiquitous surveillance pose significant threats. Investments in technologies, policies, and practices should be aligned with democratic values to safeguard privacy and sovereignty. In the military realm, access to information remains crucial, but its use on RF spectrum and global information infrastructure also exposes vulnerabilities that adversaries might exploit. As such, there is an urgent need to educate both civilians and warfighters about these risks and to balance these risks against potential successes. Fear, uncertainty, and doubt surrounding high-tech concepts should not deter us from leveraging critical technologies. Therefore, focusing on the wireless domain is critical, given its transformative potential for various industries, including the battlefield, and to maintain our continued dominance in these arenas.

### **SUMMARY KEYWORDS**

brightest minds, capabilities, create, DoD, ensure, including, information, likes, localization, networks, *Neuromancer*, Orwell, people, proprietary vendor, research, supply chains, technologies, transformed, work, world

### **TRANSCRIPT OF RECORDING**

“The sky above the port was the color of television tuned to a dead channel.” That’s the opening line from one of my favorite books, William Gibson’s *Neuromancer*. The story of *Neuromancer* takes place in around the year 2035, but isn’t it interesting that by then most of us won’t even remember what a dead channel on a television means? Here’s another famous opening line from George Orwell’s *1984* - “It was a bright day in April and the clocks were striking 13.” Both *Neuromancer* and *1984* are dystopian novels said about 50 years past when they were written. Both novels have a profound impact on how we think about technology, cyberspace in the case of *Neuromancer* and surveillance technologies in *1984*. But, to finish off my quotes for this talk, as another science fiction author Cory Doctorow likes to say, “these books are intended as warnings, not suggestions.” I often find it instructive, important even, to learn from authors like these. It’s easy for me to get complacent, just thinking about technology. What a good science fiction author can do is help us understand how technology impacts people, societies, and cultures.

Hello, my name is Tom Rondeau, and I get to be the principal director for the future G and 5G office for the U.S. Department of Defense, serving the office of the Undersecretary of Defense for Research and Engineering, or OUSD(R&E). For those who don’t know, OUSD(R&E) is the primary adviser to the DoD on all matters pertaining to technology development, transition, development of prototyping, experimentation, and administration of testing ranges and activities. As the principal director of the future G and 5G office, I am responsible for research funding and execution of programs to advance warfighting capabilities using 5G and future generation wireless technologies.

So, let's try to imagine the world of 2035. In this world, we are currently on the sixth-generation mobile system for wireless communications. In fact, we're already sick of discussing 6G by 2035 and are deep into the discussions about 7G. But 6G is where the markets have caught up with the visions of our current 5G goals. It has afforded us new capabilities, which previously were not available. Not just AI/ML, but native AI/ML that is built into the air interface and every processing layer in the network, enabling what DARPA likes to think about as contextual learning. 6G is green technology, it has given us better energy efficiency and sustainability. We now have transformative, extended and augmented reality - or AR/XR services, which resulted from the combination of ultra-low latency and ubiquitous coverage necessary to create useful and reliable applications.

Other expected trends in 6G include seamless global connectivity. This will be accomplished between terrestrial deployments across any densely populated areas, and non-terrestrial networks or NTN, connecting us everywhere else. We will have integrated sensing and networking, which will mean more knowledge about our environments and the needs to create context-based solutions. And hyper localization services down to the centimeter, if not millimeter, of accuracy, opening up whole new ways we will engage with the cyber physical world. Leveraging these big capabilities, I just mentioned will lead to innovations like better AR/XR capabilities baked into everyday devices, even contact lenses. Perfectly orchestrated and secure supply chains. Remote medicine in any environment in combat at home and out at sea. Zero touch provisioning to create the responsive and autonomous integration of computation and networking to meet dynamically changing needs. We'll have highly capable intelligent agents acting on our behalf. Collaborative robotics that will combine different skill sets and capabilities to solve increasingly complex problems. Autonomous network vehicles to automate traffic controls and improve congestion, while reducing accidents.

Our previous work in 5G solved many issues plaguing the DOD and laid the groundwork for 6G preparations. Some of these accomplishments included: outfitting and optimizing all DoD installations and sites with 5G capabilities, setting the stage for 6G by having developed in-house 5G expertise. We developed relationships and processes for working with nontraditional providers, creating stronger collaboration between commercial tech firms and the defense industrial base. Our collective work pushing the development of open, nonproprietary networks resulted in robust, end to end secure supply chains and we eliminated proprietary vendor lock through a work in open RAN.

Our work at Norfolk transformed the way we move data Ship-to-Shore, improving logistics, particularly with refit time for air assets, as well as organic ship needs. DOD critical infrastructure is now composed of both private and public networks working together through the collective efforts of many of our 5G research programs. Through our applied research at Joint Base San Antonio, we have extended medical expertise with real time connections to expert advice and guidance for our warfighters.

We now have many capabilities we did not previously have, including rapid network assessment tools to monitor the trust of networks encountered by our warfighters. Resiliency tools we leverage 5G to steer traffic to multiple places. Integration and widespread deployment of edge computing. Distributed, dynamic, resilience, and on-the-move command post and operation centers. Through our work in 5G and now with new capabilities afforded by 6G, we are able to perform at the same level or better as 5G, using less energy and manning - think ubiquity across all platforms. We will further strengthen our partnerships with the private sector through secure slicing and dual-use technologies. With the power of 6G and through the use of AI, we will have self-manning systems.



But with this new generation, there are always drawbacks and concerns. This is where the voices of the likes of Gibson and Orwell play an important role in understanding the consequences of our technologies. Cybersecurity risks will remain a problem, and the increased information being collected, transmitted and processed within our networks will continue to grow. Novel attack surfaces will appear with the improved localization technologies. Imagine how much information you might give away if your network is tracking your movements down to the millimeter level of accuracy. Ubiquitous coverage means the potential for ubiquitous surveillance. We need to be investing in technologies, policies, and practices to minimize the threats to our privacy, and sovereignty. In other words, we need to imbue our technologies with our democratic values that oppose oppressive autocracies.

And these issues matter for the warfighter. Not just what they are fighting for, but how they're able to win. Access to information is a critical warfighting concept, yet that access, including our use of the RF spectrum, and our presence on the global information infrastructure are also potential targets to deny, degrade, deceive, influence, and exploit our people on the battlefield, in the command post, and back to the decision makers in the field or at the Pentagon.

We will also need to ensure that we have educated people in the DOD, civilians and warfighters alike, that understand the risks, but also how to balance those risks with success. Fear, uncertainty, and doubt are easy to sow with high tech concepts. A lack of understanding can lead to decision paralysis or avoidance of critical technologies for fear of a single flaw.

In closing, I would like to encourage you, some of our nation's brightest minds, to seriously consider focusing your attention on the wireless domain. Wireless is not only transforming how all of our industries and verticals do business but will also significantly transform the battlespace. Ensuring our warfighters get the information needed to execute their mission has always been a critical advantage to an operation. The advance of information and communications technologies only increases the need to innovate and ensure our continued dominance on the battlefield.

It is my hope that with our efforts at the future G and 5G office, along with the efforts of the people in this room, we will work together to mitigate these threats to ensure country safety along with the safety of our allies. Thank you."

## **SPEAKER E - DR. COLLEEN JOSEPHSON | NEXTG ALLIANCE**

*Thu, Mar 30, 2023*

### *Summary*

The third industrial revolution, spurred by the advent of modern Information and Communication Technology (ICT), has significantly transformed societal norms. Mobile communication networks have played a pivotal role in this revolution, with 83% of the world population having access to mobile broadband as of 2021. However, there are significant challenges, including a lack of broadband access among 43% of low-income Americans. Internet access, once viewed as a luxury, has now become essential, with the COVID-19 pandemic emphasizing its importance for sustaining economic and social activities. The societal and economic needs working group aims to identify and characterize the social and economic drivers of the NextG technology, drawing on Environmental, Social, and Governance (ESG) assessments, and the United Nations Sustainable Development Goals (SDGs). The group has prioritized five key outcomes - digital equity, trust, sustainability, economic growth, and quality of life.

Digital equity, ensuring that network services are financially affordable, and geographically available, is essential to mitigate societal unrest and violence. NextG systems must be trusted, ensuring data privacy, security, and resiliency to recover from attacks or natural disasters. Emphasizing sustainability, NextG systems should minimize their environmental Footprint, while enabling sustainable practices across other industries. Economic growth, stimulated by innovation and efficiency, should be encouraged, necessitating conversations between industry leaders, policymakers, and defense stakeholders about spectrum access. Lastly, NextG should enhance the quality of life, improving public services, such as healthcare and education, while ensuring human rights, freedom, peace, and democratic values. The relationship between NextG and societal and economic needs necessitates strategic national efforts, improved stakeholder collaboration, and market structures that support digital equity, trust, sustainability, economic growth, and quality of life.

## **SUMMARY KEYWORDS**

access, applications, communication, creating, economic, economic growth, education, information, life, network, outcomes, privacy, quality, security, sensing, societal, sustainability, technology, trust, world

## **TRANSCRIPT OF RECORDING**

"Hello, my name is Colleen Josephson, and I'm an assistant professor of Electrical and Computer Engineering at UC Santa Cruz and a senior research scientist at VMware. I currently serve as the chair of the societal and economic needs working group in the ATIS NextG Alliance. I'm also co-chair of the Green G Working Group, which focuses on wireless sustainability. My technical background is in low power wireless communications and sensing with a recent focus on how these technologies pertain to environmental, economic and societal sustainability.

The advent of modern information and communication technology (or ICT) ushered in the so called third industrial revolution, and has transformed the way that our societies work, play, and interact. Mobile communication networks have been a key part of this revolution. As of 2021, 83% of the world has access to mobile broadband. Wired broadband lags that figure significantly - less than 20% of the world has access. We might think that a wealthy nation like the United States is immune to these challenges, but that is not the case. An astonishing 43% of low-income Americans lack access to broadband.

Once viewed as a novelty, internet access has become essential to our society's daily life. The ability to access the internet via mobile networks has demonstrated the potential to transform the societal and economic prospects of people both in the U.S. and around the world. Modern Information Technology provides people with information regarding market conditions for the crops they grow and the products they sell. Societal and political movements benefit from the ability of modern information technology and mobile telephony to organize effectively on both a national and transnational basis. Education opportunities can be made more accessible as teachers and students reach each other using applications that create virtual environments.

Indeed, it can be argued that the COVID-19 pandemic, as serious as it has proven to be, would have had an even more dramatic social and economic effects had internet connectivity not been available widely throughout much of the world.

The societal and economic needs working group has been working to identify and characterize the NextG social and economic drivers, and to make recommendations for how these factors should influence the NextG prioritization for North American research, development, and deployment. Our approach is to identify and prioritize relevant societal and economic issues, as informed by environmental and social governance - or ESG, materiality assessments. We are also informed by the United Nations Sustainable Development Goals or SDGs. The SDGs were introduced in 2015 and have been adopted by all United Nations member states. They've also been adopted as guidelines for the area's NextG alliance working groups. The goals act as a shared blueprint for peace, prosperity, and people on the planet for now, and in the future. They cover 17 areas spanning topics such as gender equality, marine conservation, economic growth, and global peace. A number of these are tied directly or indirectly to mobile network connectivity.

During our working groups first year, we established a base inventory of social and economic issues and then group them into five outcomes - digital equity, trust, sustainability, economic growth, and quality of life. I'll spend some time defining these outcomes and discuss how they relate to NextG and our nation's potential future defense priorities. First is digital equity. This is achieved when the following three conditions are true for each user: financial affordability, physical accessibility, and geographic availability of network services. As I mentioned earlier, digital equity is far from reality in the United States. Inequality creates rifts between different parts of the population, leading to unrest and in some cases, even violence. Therefore, to ensure a safe and peaceful society, it's imperative that all Americans get equal access to the transformative power of technology.

Trust. Looking forward, leaders in the 6G space are envisioning ultra-immersive user experiences such as VR, XR, and even brain computer interfaces. Advances like smart surfaces could weave IoT devices throughout our homes and businesses, and even things like smart clothes or medical devices could end up in, or on our bodies. These devices handle inherently high sensitivity information that if mishandled, would grant observers unprecedented insight into the behavior of American citizens and institutions. Thus, NextG systems must be trusted by governments, corporations, and civilians to the greatest degree possible. Key components of trust include security. NextG needs to ensure that information is securely and reliably delivered between endpoints. The network itself needs to be secure against external attacks, and resilient enough to go into recovery mode if attacks occur. AI-related gadgets and sensors serving digital automation if critical processes should mandate trustworthiness, resiliency, and security.

Data privacy. The vast volume of personal data being generated and tracked introduces privacy and ethical use concerns around what kind and quantity of information is being passed, and to whom. At the intersection of security and privacy, one particularly concerning possibility is the ability to observe and manipulate users' information streams without authorization. When paired with the highly immersive technologies like VR, XR, and brain machine interfaces, we're suddenly upon a future where it could become possible for bad actors to literally change how people perceive the world. Therefore, it's absolutely necessary to protect network integrity and ensure the privacy of user data.

And finally, resiliency. NextG systems need to be highly resistant to disruptions and operate in an acceptable degraded mode if damaged by malicious attacks by humans, or natural disasters like fires, floods, and other instances. A reliable and resilient network is essential for supporting national critical infrastructures.

The third outcome is sustainability. Climate change has led to an increase in extreme weather events that endanger the life and livelihood of U.S. citizens. We've come to understand that technology has a considerable and growing impact on the world. The carbon footprint of the ICT industry is actually on par with that of the aviation industry. And unfortunately, it's projected to grow significantly in the next decade if substantial preventative action isn't taken. Thus, as we begin to design NextG, it must be inherently sustainable in a way that previous G's have not been. Furthermore, it's desirable that NextG systems are not just climate neutral, but that they also enable sustainable practices across other industries. NextG enables smart agriculture, for example, will help ensure food security by maximizing crop yields, while minimizing resource consumption.

Economic growth. NextG is expected to encourage economic growth by increasing productivity, innovation, efficiency, effectiveness, and creating new value propositions, business models, and market segments. One particularly interesting intersection of defense needs versus supporting economic growth is the challenge of spectrum access. We've witnessed free and open access to unlicensed spectrum and the ISM band led to groundbreaking technologies like Wi-Fi, ultra-wideband localization, and low energy communication via BLE, ZigBee and other technologies. However, different parts of the spectrum enable different applications. So, for example, millimeter wave spectrum is capable of achieving rapid data rates and high-resolution sensing applications like gesture detection. That same range of spectrum is completely inadequate for agricultural sensing, which would rely on longer wavelengths for long distance signal propagation, or applications like underground sensing. Therefore, to maximize economic growth and innovation, while maintaining national security, we will need to have a series of conversations between industry leaders, policymakers, and defense stakeholders.

Finally, quality of life. NextG will be important for improving quality of life in all of North America and its local communities, including for public services, such as health care, education, safety and security, and the environment. It could also potentially benefit human rights, freedom, peace, and democratic values. As we look to enhance quality of life via applications like telemedicine, and remote education, and enhance public safety, we need to maintain the balance between the benefits that these technologies provide and the vulnerabilities they could expose us to. Thus, quality of life is often strongly linked to other outcomes, such as economic growth and trust.

I hope that this overview has been useful. Looking forward, my experience chairing the societal and economic needs working group, has shown me that the relationship between NextG and societal and economic needs is a rich topic that demands national strategic efforts. Improved channels are needed between stakeholders throughout government, industry, academia, and elsewhere. This will allow the necessary interdisciplinary collaborations and research and development, defining of required metrics, and support of market structures that will be required to make America the leader in creating NextG technologies that support digital equity, trust, sustainability, economic growth, and quality of life to the fullest extent possible."

**SPEAKER F - DR. JONATHAN M. SMITH | PROFESSOR, UNIVERSITY OF PENNSYLVANIA**

*Tue, Feb 07, 2023*

*Summary*

The economics of the wireless carrier business are driving a shift towards "softwarization," fundamentally changing the way networks operate and are managed. The internet's success has made much of the wireless network infrastructure rely on internet packet format data, making a significant departure from the traditional telecommunication industry model. While 5G networks have brought changes in both phone frequencies and infrastructure, the latter is more crucial for the transition to 6G. Higher throughputs, largely driven by the demand for high-quality media streaming, necessitate a greater wireless channel capacity and edge computing, where computation is done close to the data source. However, this approach introduces challenges in controlling complex software running on numerous remote devices, an issue pertinent to both 5G and 6G. Moreover, higher frequency signals have greater attenuation, requiring more base stations to ensure coverage.

In the transition to 6G, there is a significant emphasis on software components, particularly machine learning-based AI to manage networks. The close proximity of computational capability to the edge of the network allows for innovative applications of AI. For example, AI can be used to select the best path for data transmission, much like how smartphones switch between Wi-Fi and cellular networks. However, such AI-driven processes can be risky, as the decisions they make depend on the data they have seen, potentially leading to catastrophic errors in complex tasks like self-driving cars. The increasing complexity of systems is believed to be the ultimate enemy of security, as understanding and managing complex systems becomes exceedingly challenging, particularly when malicious actors can exploit overlooked assumptions in system design. IoT further complicates the landscape, introducing a plethora of unmanaged and unfamiliar device types. The management of these complex 6G networks, populated with edge boxes running inexplicable AI, presents significant challenges and threats.

**SUMMARY KEYWORDS**

AI, complexity, control, data, device, edge, frequency, higher frequencies, infrastructure, internet, means, network, problem, profusion, provide, services, software, system, users, wireless carrier

**TRANSCRIPT OF RECORDING**

"First, it's important to understand what's going on in the wireless carrier business space. The way I see it, economics is driving what is called softwarization. You have to think of the roles that various business entities play in funding and building technological advances.

The success of the internet meant that much of the underlay that supports the wireless network is really internet packet format data. So, it's not part of the public internet, but it uses internet technology. However, this is a fairly radical change for several reasons. One is that the telecommunications industry often views the world as being customers and us, and so, the model is that if they have a boundary line between the service they provide and the infrastructure that they use to provide it on, this was learned through experience. But basically, what's happened is that in 5G, everything changed.

But there's potential confusion between the use of 5G frequencies in phones and the 5G infrastructure. The infrastructure is much more relevant to the 6G transition. So, generally there are desiderata that people have from our wireless service as an increasing number of people, you know, move around big images and watch video on their smartphones there's a demand for higher throughput.

And throughput is driven by a couple of things. One thing is the capacity of the wireless channel, and the other is the ability to achieve service from the services that are being requested, say a video streaming application. Now, what you have in the case of a 5G network is the frequencies - because they are auctioned, are in use; however, much of the envisioned software infrastructure, for example, there is a model of computing put at the edge of the network - meaning, you could think of it as being computing co-located with the wireless access points.



Now, that, that means that the control loop cannot be cross country. Some of the delays that have been promised you know, say 50 milliseconds or less for an edge service, means that these edge computing capabilities have to be close to the users.

So, now you have complex software running on many, many boxes that are really not as easy to control as they would be if they were in an office tower in a major city. That's as true of 5G as 6G. Higher frequencies have problems with matter, like us, you know, we look like a bag of salty water to a radio transmitter - we provide about 6dB of attenuation. This variation of our signal strength, it worsens even more for higher frequencies. That means that you have to populate more footprint with base stations in order to provide coverage to mobile users.

Let's look at the software component for a minute because that is going to be a key threat in my mind. What you can imagine, and this is one of the key differentiators between 5G and 6G, that having the computing capability close to the edge of the network and new users allow you to think about things you can do with computers. So, one of those is the use of statistical machine learning. So, proposals are on the table to essentially have AI do network management. The big problem with using statistical machine learning-based-AI is that you can build lots of self-checks that wrap-around the AI, but the problem is that any decision-making process based on big data is subject to the data that it sees or has seen. So, there are risks where the, you know, the routing, and other decisions made by the AI could go awry.

The interesting pathfinder, that many of us use it on a daily basis, is the Wi-Fi cellular sharing on our smartphones, because what it does is it tries to use the best path to send data. Typically, you configure this with the cellular assist. 6G generalizes this idea and it does this because the complexity is much, much greater in the spectrum, and that's a good way to spend some of the computational capabilities in the edge devices. However, AI can create a big threat vector. One of these being that you can have it miss trained, so that it might not correctly discriminate between say, you know, a toddler and tumble weed in a self-driving car with all kinds of disastrous consequences.

It's generally believed, and I believe it will further that complexity is the ultimate enemy of security. Because a complex system is hard to understand. And if you understand what you need to make it work, that's usually where folks leave it. But if you have a different objective, if you're an adversary, what you will look for is unexpected behaviors that will throw the system into an unwanted state - basically, violate all the assumptions that the designers made. In complex systems, there are so many assumptions that you can almost certainly find one that's violated in, you know, in the context of use of the system.

So, not only do you have more complex software running in the network control plane, but you have more elements, more administrative barriers, companies, etc. That I think is the, you know, the biggest potential threat.

One that I'll bring up that I'm particularly concerned about, because I don't think that people have a complete handle on exactly what the implications are, is what's called the Internet-of-Things. What I am concerned about with IoT is, again, a profusion of unmanaged and unfamiliar device types. It's not a phone handset anymore. You know, it's a world of software. The risk is, if we look at defense in particular, that you know, we use commercial products and infrastructure, and complexity is rampant. And you know, I can't think of a configuration management strategy that would be adequate to allow us to check all of the boxes that we would want to for a 6G network with edge boxes running AIs that we can't explain and don't understand, and opportunities for espionage and availability attacks of a scale, and nature that we've not seen before."

## **SPEAKER G - DR. ANG CUI | CYBERSECURITY RESEARCHER**

*Wed, Apr 05, 2023*

### *Summary*

6G is envisioned to have significantly more bandwidth, with everything from pixels to doorknobs connected to a global network. However, instead of discussing potential threats, it's more useful to consider the future dynamics in a 6G world, particularly the adversarial dynamic. In this context, the simplest dynamic involves two adversarial groups - defenders (the good actors controlling resources) and attackers. Focusing on a quantifiable resource, like cumulative bandwidth under control, it's evident that the power dynamics have changed over time. In 2005, defenders controlled most of the bandwidth. However, by 2023, attackers have managed to control more cumulative bandwidth than any single defender, mostly due to the insecurity of devices on the edge. A clear example of this power shift is the Mirai Botnet Attack.

Projecting this dynamic into the future and considering compute power as a resource, there's a likelihood that attackers may also control more of this resource than defenders. In this scenario, attackers could leverage AI learning algorithms and other compute-intensive technologies against us. The implications are dire, from on-the-fly deep fakes that compromise trust in digital interactions to attackers having more control over our perceived reality than defenders can counteract. The future of 6G will hinge less on bandwidth and frequency, and more on who controls the edge devices. Preventing a future where adversaries control our edge resources is the key to ensuring a secure 6G world.

## **SUMMARY KEYWORDS**

adversary, attacker, bandwidth, botnet, call, compute, control, crossed, cumulative, defender, devices, disposal, dynamic, edge, fundamentally, future, hopes, point, resource, talk

## **TRANSCRIPT OF RECORDING**

"Hello friends! My name is Dr. Ang Cui, and let's talk about Threatcasting 6G. So, last time I checked 6G doesn't really exist, I think it's a lot of hopes and dreams. And when I dream and hope about 6G, I think about a future where we have a lot more bandwidth, of course. Every device, a lot of nonsense devices, and also some more important ones. Every single pixel, every doorknob, every switch, everything, is going to have an incredible amount of bandwidth at its disposal, and all connected to a global network, and all of our dreams are all going to come true.

Okay, so, instead of talking about the potential threat of our hopes and dreams, which you know, is dark, let's talk about what the future you know, in a 6G world might look like. And more importantly, let's think about adversarial dynamic. Let's think about the evolution of that dynamic between now to 6G, and maybe even beyond that, right? So, we're going to be looking at a few graphs. So, let's keep it simple. Let's look at this graph. Here, we're going to talk about the simplest of dynamics; we have two adversary groups; let's call the blue - the defender, and the red - the attacker. Okay, and we're going to focus on one "resource" at a time. Now, resource can be anything from time, money, happiness, bandwidth, CPU, whatever it is. It is a quantifiable resource that can be controlled by the defender or the attacker. And then on the x-axis, we're going to have just time, right? How does this change over time? So, let's take the resource A, and let's go back a little bit in time. So, look at this adversary dynamic starting from 2005 to 2025, and maybe even to 2035. And let's call resource A - cumulative bandwidth under control. So, we're talking about all of the bandwidth that is controlled by the defender, versus all of the bandwidth that is controlled by the attacker, in some capacity.

Okay, so in 2005, if you think back to like, Blackberry days, right? A lot of the bandwidth is controlled by the defenders, good people like in the core of the network. And then as we go from, you know, that time to maybe like, I don't know, 2014/2016, you know, something happened. Like a little weird thing. And then as we crossed that point to 2023, I would argue that it is pretty much settled that the attackers control more cumulative bandwidth than any single defender can possibly have, right? Even all of the cumulative bandwidth in every data center controlled by any single entity. And that's because all of the devices on the edge are insecure and have been taken over by the attacker. And if you think about all of the bandwidth on the edge, right? There's a whole lot more of that, than any single defender can have.

Let's look at this graph. So, we start out in 2005, the defenders have most of the bandwidth, right? And as time moves forward, we have more and more of these computers that are on the edge that are insecure, that are controlled by the adversary. And at some point, the blue line crosses with the red line, that intersection point, right, is the point where every scenario dynamic fundamentally changes, right? Where the defender used to have the advantage, now the attacker decidedly has the advantage, at least within respect to that one resource. Now, when this line crossed, guess what happened? There was a little thing called the Mirai Botnet. Mirai was the first botnet that mostly used embedded devices on the edge - like your home router, your webcam - and it was able to gather up the largest denial of service attack the world has ever seen. And fundamentally, that's the point where we crossed that intersection - where red became larger than blue. Let's think about some other resources that we can replace with just bandwidth.

Let's call it compute power, right? And compute power I'm going to classify as the cumulative amount of slack CPU and slack memory that is available to A - the attacker, and B - the adversary, will move the timeline forward. And in this case, I also think that at some point, the blue line is going to get crossed by the red line. So, what happens in a future where the attacker fundamentally controls more compute resource than the defender can ever have?

Let's think about what that means. All of the things that we use today to sell more socks and, you know, advertise on the internet, all of the things that are available to us that require compute power AI-learning algorithms, and such. Well, guess what? The attacker can use that too. And in a world where the attacker fundamentally controls more of resource B than the defender, I would think that the attacker would have a decided advantage in terms of machine learning versus the defender. Now think about what that future will look like.

The future where fundamentally, attackers have more compute resource at their disposal to learn against us than all of the defenders have, in terms of resource to learn to protect us. What does that world look like? Well, every time you talk to a human being, you interact with media in terms of video and voice. And any kind of interaction where we can have deep fakes on the fly, right? A future where we can't actually trust any kind of video footage because it very much can literally be a deep fake-generated from the device firmware itself, versus the thing that actually happens. What happens to traffic cameras? What happens to nanny cams and security cameras of all kinds? What happens to every telephone call? Every human interaction that is literally now face-to-face, we are going to fundamentally step into a future where the adversary has more compute and more control over our perceived reality, then the defenders can help us have.

Let's bring home - Threatcasting about the future of 6G. It's not going to be about: the bandwidth; the frequency; if we're in space; or in the ocean; or in the sky; or on the ground. The future where the defender wins in a 6G world depends on who controls the devices on the edge. If we fundamentally can't control the edge with all the resources that we're putting into it, we're going to lose the future. So, let's talk about how to prevent a future where we create all the resources on the edge and hand it over to the adversary and then lose for years to come."

## **SPEAKER H - DR. JOEL MOZER | TECHNOLOGIST**

*Wed, Feb 22, 2023*

### *Summary*

As the U.S. Space Force reflects on its first three years of existence, it's evident that our world is on the brink of a transformative era in space technology. Currently, our focus is on data collection and communication, supporting terrestrial operations and safeguarding U.S. interests in space. However, the rapidly evolving space enterprise, demonstrated by initiatives like NASA's Artemis program, Elon Musk and Jeff Bezos' ambitious ventures, space tourism, and in-space manufacturing, signals exponential advancements in the space domain. These developments, along with the proliferation of microelectronics and sixth-generation wireless communication, have made space increasingly accessible to governments, companies, and private individuals. The value of the space economy, estimated at \$450 billion per year worldwide, could balloon to \$4 trillion by 2035, and as the cost of space access diminishes, we may see an increased human presence in space.

Facing this evolving landscape, the U.S. Space Force must prepare for an expanded future, which will likely involve next-generation communications like 6G. In this hyper-connected world, we will have access to an unprecedented amount of real-time data, enhancing our battle management and space situational awareness. With the aid of AI and machine learning, we can potentially eliminate the fog of war altogether. However, our competitors and adversaries will also have access to these resources, heralding an era of informatized and intelligent warfare that necessitates new strategies. Advanced communications and ultra-low latency will enable new operations, such as off-boarding calculations for individual spacecraft or swarms, further optimizing resource use. By embracing these technological advancements, we can ensure the U.S. maintains its leadership position in space activities, ready for the challenges and opportunities the space sector will present in 2035 and beyond.

## **SUMMARY KEYWORDS**

6G, advancements, AI, architectures, artemis, challenges, communications, connectedness, data, economy, future, interests, latency, launch, manufacturing, microelectronics, space, tourism, warfare

## **TRANSCRIPT OF RECORDING**

"Ladies and gentlemen, it is my pleasure to speak to you today about the United States Space Force and the future of space and space-related activities that will be affected by Next Generation Communications Technologies. Today, the space force is all about data and Communications whether it is our satellite communication; Mission our position navigation and timing; Mission our space situational awareness; Mission or our intelligence surveillance reconnaissance or missile warning missions our business is collecting data and communicating it to those who need it when and where they need it most. But you know, we are in a hinge of History moment with respect to space and space technology today. You only have to pick up a random news feed to see that we are the knee on the curve of exponential advancements in just about every aspect of space today - whether it's NASA's Artemis program to return humans to the surface of the Moon, the advances made by Visionary industrialists like Elon Musk or Jeff Bezos, or the rise of space tourism and in-space. Manufacturing the space Enterprise is clearly growing in amazing ways.

Another indicator of the growing space enterprise is the existence in the United States Space Force itself, established just over three years ago, the Space Force supports the joint terrestrial fight, but also has the mission to protect U.S. interests in space; no matter what they become, this requires us to get ahead and stay ahead of these exponential trends in the space domain. This includes related technologies, such as ever smaller and more capable microelectronics and a sixth generation Wireless Communications economy is estimated at about 450 billion dollars per year worldwide.

The possible scenarios of space over the next couple of decades include much more economic activity. Some estimate by 2035, the space economy will be worth four trillion dollars every year. Today, there are only a handful of people who live and work in space, but in the future, there may be more people, perhaps thousands. One trend that we see clearly already today, is that space is no longer reserved just for superpower governments. There are many more players from governments, companies, and even private individuals going to space, and that trend is expected to continue, especially as the cost associated with space access goes down dramatically as we look ahead to 2035. We must plan for an expanded future, including one with Next Generation Communications, such as 6G because the United States space force is tasked with protecting U.S. interests in space and it's vital that we plan for this expanded future, so we can ensure to continue to protect our nation's interests in space will be one element of a hyper-connected world, along with 6G Wireless Technologies.

We will have access to more data in real time than ever before in history. This connectedness increases the Space Force's ability to support battle management and space situational awareness around the world. New proliferated intelligence capabilities across the electromagnetic spectrum will produce more data than we can currently handle with present Network Technology by leveraging large data sets and AI/ML techniques. We could potentially reduce or eliminate the fog of war effect altogether.

This will be a game changer for warfare across the board, as 6G technology spreads our competitors and adversaries will similarly have access to more data. This informatized and intelligent high warfare will require new ways of thinking and new strategies. To compete, we must be prepared to meet the challenges of this new era and leverage our technological advancements to maintain our position as leaders in space activities.

Ultra-low latency communications will enable new concepts of operation in space. For example, it will allow the off-boarding of calculations for individual spacecrafts or even swarms of spacecraft for activities, such as rendezvous and proximity operations. Some of this competition will be done on the ground, but some of it will be done with supercomputers. Stationed in space, these new architectures will require new communications and will allow for more efficient use of resources, and enable us to achieve our goals more effectively. The coupling of low-cost reusable launch ever more capable microelectronics and next generation communications links will lead to amazing and disruptive capabilities. In the space domain, we must be ready to embrace these advancements and leverage them to advance our nation's interests. In conclusion, space activities in the 2035s and 2045s are expected to be vast and much more advanced than they are today. We must plan for an expanded future, including one with next generation communications, such as 6G, as the United States space force continues to protect U.S. interest in space. We must be prepared to meet the challenges of this new era and leverage our technological advancements to maintain our positions and leaders in space activity. Thank you very much."



## **SPEAKER I - ANTON MONK | VIASAT**

*Mon, Apr 03, 2023*

### *Summary*

The current focus is on using both GEO (Geostationary Orbit) and LEO (Low Earth Orbit) satellites for narrowband applications, primarily for messaging and potentially voice transmission. This capability can improve the situational awareness of soldiers on the battlefield and enhance communication back to command. There are challenges, such as how many users can be supported and ensuring quality of service (QoS), particularly in the harsh environment of the battlefield. Another challenge is ensuring the security of these networks, which were not originally designed with satellite transmission in mind and are thus not optimized for this purpose. However, by using small, low-cost, and standardized devices, a form of security can be achieved through a 'hiding in plain sight' approach.

Additionally, the integration of 5G or 6G networks could facilitate seamless connectivity across multiple orbits, bands, and satellite operators, creating a more resilient network. The challenge lies in how to adapt commercial satellite technology for defense purposes without incurring high costs for custom-built solutions. Furthermore, the increased use of space brings concerns around space sustainability and regulation. As more entities are launching satellites, the risk of collisions and subsequent debris increase, which could jeopardize space utilization for everyone. This leads to a need for better regulation of space and attention to orbital debris concerns, all of which will impact the future of satellite-based communication and 5G/6G technologies.

### **SUMMARY KEYWORDS**

applications, area, band, collisions, commercial, concerns, devices, geo, IoT, LEO, messaging, network, operators, satellite, security, solutions, space, spectrum, support, terrestrial

## **TRANSCRIPT OF RECORDING**

"Almost everything that's happening now is narrowband. And that can actually, even though the discussion has been around layout LEO, it can be supported with GEO. And that's where Viasat's interest comes in. And I'm going to transition for a second to talk about different types of spectrum because that really is a critical area. How do you use the spectrum? There are two areas of spectrum; two areas of bandwidth capability. Let me finish with that first, actually. So, for the five megahertz, you can't really close the link to GEO satellite. The big promise is that you could get 10, 20 plus megabits-per-second direct to your handset from a satellite. That's very challenging, even for LEO. And even if you can achieve it, like some are promising, the question is how many users can you actually support? So, realistically, for some time, the use case that we're talking about is messaging, and potentially voice. And just those two alone, we believe can provide dramatic improvements in the view of the soldier on the battlefield. What information, situational awareness can be transferred back to headquarters, or command?

So, as I mentioned, this can be done both to GEO and to LEO. The advantage of GEO is those solutions out there already. And LEO solutions are still evolving. They are very expensive. Many of them are custom built. The LEO layer solutions will evolve, but the big advantage of standards is you don't have to make a decision. Do I do GEO or LEO?

It's a standard. It's like you don't have to decide if I talk to an AT&T network, and I go overseas, and I connect to a Vodafone network, they've got some relationship where I can roam. We expect that 6G, or even enhancements of 5G, will enable the same capabilities. You have a connection to a local terrestrial operator; you move out of coverage; and your phone will connect seamlessly to the satellite network, albeit with different capabilities.

Other types of devices that we think are super interesting for these battlefield type applications are what are currently called puck devices - they are similar to MiFi devices. And they either have Bluetooth or USB for added security to the phone (any phone). A messaging app. Then an IoT-type connection directly to the satellite. That means you can have these small \$100 type devices, which actually will be rolling out in the commercial sphere (initially in Europe), and then probably later this year in the U.S., - that can enable any phone, even legacy phones as long as they have the app, that works with these pucks to talk directly to satellite - for these messaging type applications.

In terms of differences between defense and commercial requirements, I think there's a few categories here. If we focus on direct-to-device, and specifically on these 3GPP messaging type applications, these narrowband IoT and LTM-type solutions are not designed, one, for satellite origins - they're not optimized. There is a lot of overhead in the protocol spec. There are companies that are addressing this by improving the efficiency. It's not a security issue, but it's just an efficiency. How many users can you support? How many messages per second can you support? Maybe a bigger area that needs to be addressed, is there's no real, there hasn't really been a need for QoS. So, if you need (or network slicing, which is another topic within 5G that hasn't really been a requirement for these IoT type applications), but now we're saying, "Okay, we're going to use them for messaging, in these mission critical applications in battlefield environments." Well, in that case, there's two areas of concern. One is security. And the other one is quality of service. And there's basic encryption like there is on any network (I think it's AES encryption), but there will need to be more done to make the network more resilient. And there's not much you can do about aspects, like low probability of intercept and detection, I think.

Certainly, these networks, just like any cellular network is a problem, not just for direct-to-devices; they're designed to be HPI, HPD - you're trying to find the network as efficiently as possible. But the advantage of small devices is, I think, they can be attritable, meaning they're so low-cost, because they're standardized. Imagine if you can get a sensor that can transmit for \$30. And you can sprinkle them around a battlefield. Just one idea of the things you could do. Before that, you wouldn't normally do with \$1,000 or \$10,000 devices, then it's hard for an adversary to figure out what's going on - you're literally hiding in plain sight.

So, I think there are ways to get around the lack of standards-based security, by sort of this hiding in plain sight mechanism. There are elements of security, I think that can be added and need to be added on top as well, and ViaSat is certainly looking at that. QoS is not natively supported, I think, to the level that it probably would want to be for these types of applications. Because, you may have messaging for soldiers that is not mission critical, and you may have others or for Generals or so on, that really need their messages to get through, or people that are out in critical environments where those messages have to get through. So, that's another area I think there are potential gaps. In terms of general 5G NTN, one of the areas that we see, for commercial applications; a lot of what ViaSat has done is focused on bandpipe satellites. We don't have satellites to do a lot of onboard processing. And the reason is because there's very limited power available on a satellite, and you want all that power going to as much of the signal as possible. Some of the new satellites that are being talked about and being rolled out have onboard processing for phased array antennas, and for inter-satellite links. So, this is somewhat related to 5G (doesn't have to be), but for 5G applications, certainly the same concerns apply.

If you want to increase resilience and support scenarios where you have gateways on the ground that are taken out (in a kind of a warfare environment), you probably want to have ways to relay the information between satellites. So, inter-satellite links become more critical for defense applications, I think, as well as potentially, not just LEO inter-satellite links, but LEO-to-GEO links. So, ViaSat, and others, have solutions that we're working on to replace the NASA tactical data relay system, which actually will do LEO-to-GEO relay. Now we're starting to talk about an aspect of 5G, or maybe 6G, that's hybrid networking. That's not direct-to-device, but this is really, I think, where we'll see the seamless connectivity in the future is orchestration of multiple orbits, and multiple bands, and even multiple satellite operators to add resilience to the network. So, you've got this hybrid networking concept that people are starting to work on. There are some companies that have orchestration software, for example. There are companies already doing inter-satellite links. There's the space BACN program within the Defense Department that looks to leverage different operators; different constellations that can do this kind of relaying.

And then you have the difference between commercial and government again, with things like you want to be able to do beam nulling, not just beam forming, but beam nulling to null out unknown adversary locations to improve anti-jam, for example. Those are things that the commercial side doesn't really care about. And so, the question is, "how can the government continue to leverage all investments going into defense solutions - sorry, into commercial solutions - all of the money going into commercial solutions, leverage that still for defense applications?" And, since we do both sides, that's an area of a significant interest for us. How do you leverage what's happening on the commercial side without making custom purpose, very expensive satellite solutions just for defense applications?

So, I think I covered ground between general sort of 5G hybrid networks and orchestration between those networks. Those have their own set of security questions around them. Because if you're now transitioning, both on the ground and in space between different networks, I think there may need to be some sort of joint coordination of security between these disparate networks; different operators. I haven't thought much about that, but that seems to be an area worth discussing. And then there's the whole low-cost, direct-to-device world, which is happening much quicker than people expected. Again, because of the standards. Because Apple really generated this massive interest; because they did this deal with Globalstar to implement SOS, initially, SOS messaging, they're offering in their in the new iPhone 14's. But what's really interesting is, what are the applications that can be supported? Can you get to 5G NR - the five megahertz that I mentioned before? Well, you would need larger arrays in space. You've got issues with larger satellites and constellations and sustainability, and multiple governments trying to stake their claim to space, which is almost becoming a land grab. That's a whole different topic of space sustainability in the 5G/6G world. Where the way things have been done before where you can get approval from the FCC and start launching satellites, for example, like Starlink has done. But other entities, maybe governments on their back feet.

So, now we're talking nothing to do with protocols, but how do you deal with space sustainability when the likelihood of collision starts increasing, and the access to space in the future becomes more of a concern? I think this is why you've seen the Chinese government announce recently, I forget the number that they were going to launch, some large number of LEO satellites into similar orbits that Starlink is doing (or reasonably close to orbits) because there's a realization that there's a limited amount of space, literally for space-based assets. And it can't just be a land grab by one company and isn't really any regulation, that global regulation, like there is for GEO satellite, orbital slots and frequencies that's done through the ITU - that same doesn't really exist for LEO satellites. So, I think that's another area of security concern. Who owns "how do we regulate space" - both from a what is allowed to be in one kind of orbital shell, as well as space sustainability?

Because if you have too many collisions, they're always collisions, and these collisions grow out of control. There is a concept called the Kessler syndrome that was postulated a while back where if there are enough collisions, that could generate more collisions, and then you get this out-of-control, kind of exponential growth, in debris. If that happens, then it threatens space for everyone for decades to come.

So, yet another area of concern, threat concern; if we don't do something about regulating space. Other countries, less so, the U.S., but I think other countries like the UK, in the past year, have really started to pay a lot more attention to this question of - how to regulate space, and to take into account the concerns of collisions, and orbital debris, and things like that. Let alone concerns from astronomers about the night sky being populated with very bright objects; that's already started to happen."

## ***SPEAKER J - MICHELLE MCCLUER | MASTERCARD***

*Wed, Mar 01, 2023*

### *Summary*

The transition from 5G to 6G networks entails significant advancements in speed, capacity, integration, and artificial intelligence capabilities. The shift to 6G allows for larger networks, increased device connectivity, and new potential for artificial intelligence. Moreover, this technological leap also streamlines communications across different channels - air, space, ground, and sea - leading to faster transmission and novel capabilities. However, this expansion and acceleration also demand a rethink in how we approach security, with the introduction of new encryption, authentication, and threat detection methods, and a consideration of how we redesign current security protocols to accommodate the changing landscape.

Addressing security in this more expansive and speedy 6G environment involves reimagining traditional security concepts, such as confidentiality, integrity, authentication, and availability. With faster data transfer and an expanded network, there are concerns about the maintenance of data security and integrity. Threats could involve manipulation of data or deceptive use of AI technology, mimicking nuanced behavior and communication patterns to confuse or mislead. As technologies grow exponentially more complex, reliable authentication becomes critical in a 6G network. Even physical elements, like light communication, could be potential targets for manipulation. Despite these challenges, the future isn't bleak. Just as malicious actors may leverage the 6G network for harmful activities, the same technology can be used proactively to secure the network and protect individuals, companies, and organizations. The goal is to use the new technology as a force for good, staying steps ahead of the threats, just as we have been doing from the 1G through 5G eras.

## SUMMARY KEYWORDS

accommodate, AI, authentication, capabilities, communication, confidentiality, enable, environment, faster, individual, interfere, network, person, secure, security controls, security, talking, technology

## TRANSCRIPT OF RECORDING

"Interviewer - So, Michelle McCluer, as you're thinking about that you got a roomful of people doing threat casting, as they're thinking about the future threats in this area around 6G, what should this group be thinking about when they're starting to model that?"

"MM - When starting to model that, I think they need to first consider, "what does 6G even do? What is the purpose of moving to the 6G network from 5G?" So, first, we're going to be making things faster, and be operating in a bigger space. So, the space expands, we're able to take on more; have more devices; more of a network capacity.

It enables artificial intelligence. So, the artificial intelligence that we see active today, that we're using on a day-to-day basis is going to look different on the 6G network. It's going to enable additional capabilities for artificial intelligence and take it to that next level.

It integrates communication. So, when we think of the different channels of communication - whether that's air, space, ground, and sea - integrating across those different channels is going to look different. It's going to become more integrated; and the communication is going to work faster; and we're going to have new capabilities, being able to transmit that information across those different channels.

And then, we need to think about how it also changes how we think about security. So, we have the security capabilities of today, but tomorrow on a 6G network, we are going to have new novel authentication, encryption, access, control, communication, and of course, threat detection capabilities.

But, with these new capabilities, we also need to think about - how can we redesign our security technologies and ways of managing security, and mitigating preparation for and mitigating security threats to accommodate these future networks. And what I mean is, we're essentially operating in an unsecure environment, which is subject to all of the traditional types of threats - big and small. So, we're in this new, faster, bigger environment. But the ways that we think about how we secure our environments of today is going to be different tomorrow. So, we need to think about 6G-specific authentication, encryption, access, control communication, and detecting those threats.

And so, when I talk about threats, I'm talking about the traditional types of threats - the concepts around confidentiality, integrity, authentication, availability, and what does that mean for confidentiality? So, if things are moving faster, and the network has expanded, are our security controls in place going to still keep our data secure? The information that we're transmitting between each other, and the new channels that we have integrated now - are we accommodating that new environment? Is the integrity the same? Can threat actors change and manipulate information? Is what we see, or what we think we see, actually what we're seeing?

Authentication - if I think I'm talking to one person or one entity, because of different criteria, or variables that are presented to me - is that actually the case? Is the newly enabled artificial intelligence now being used maliciously, or deceptively, to make me think I'm seeing one thing, when in fact, I'm seeing another thing or communicating with another thing, not realizing it, because it looks so real? And I'm not just talking about looking real, but even down to those very nuanced behavioral markers that if I know that I'm talking to a specific individual - make me think of that individual - how they, you know, grin when they're smiling at me, or specific words that they use. Do they use big bridges between thoughts and their sentences that just resonates with me, subconsciously, to help me know that this individual is who they say they are? Can those then be duplicated or replicated by artificial intelligence technology? And, of course, authentication.



So, how do we present who we are in a way that can actually be validated on a 6G network compared to what we're doing today with 5G? The technologies are going to become exponentially more complex, and they're going to be relying on each other, and they're going to be interoperating with each other. And how do we keep that reliable ability to authenticate the person on the other end of that technology, who's actually requesting or sending information. How do you know that, that is the person or entity, or device that you think you're talking to, is actually what you're talking to?

And so, I think we're going to need to think through different ways of securing our technologies through new access control systems, and what those access attacks might look like. And I've even been talking to some folks here on the security research team about visible light communication, and just what we see, could potentially be manipulated. And we're talking about the quantum aspects. And again, that speed and the aspects of enabling artificial intelligence.

And how could that then interfere with things that we just don't even think of as being technology, necessarily? But, when you're looking at a television screen, looking at your phone screen - if I'm sitting on one side of a table, and you're on the other side of the table, but there's light coming down from the light bulb - can someone interfere with that light (those light waves) and make me see something different?

And so, these things may seem very sci-fi and super futuristic, but by 2030, we're going to be stepping into a (for real) 6G network, and all of these different aspects need to be considered. We have to take it back to a design and infrastructure architecture perspective and continue to, as we learn what 6G will actually look like, in the future, continue that feedback loop of incorporating new security capabilities. And what a fortunate thing is that, while the bad guys may have access to the 6G network and be able to perpetrate attacks faster and on a larger scale, and do things that we haven't even thought of yet related to malware and deep fakes, and just all of the criminal behavior that can take place on that type of network - we will also have that capability from a force for good perspective. And securing the network and being able to protect individuals, companies, organizations, etc.

So, as long as we keep that in mind that it's not a doom and gloom situation and that we have the same capabilities, as the good guys, that the bad guys do, then we will continue just like we have. Through 5G networks, we've been able to predominantly stay ahead of the bad guys and we'll be able to continue in that vein - we'll be able to continue to stay steps ahead of them and use that new technology as a continued force for good and protecting the network."

