An Introduction to Fifth Generation Warfare

The Radio Research Group ⋮ 24-31 minutes ⋮ 3/31/2022

Graduates of the 80th Training Command PSYOP class receive regimental crest pins at the end of their field exercise at Fort Hunter Liggett, California, Feb. 6, 2019.

How I Learned to Stop Worrying and Love 5GW

We type these words travelling through the Swiss Alps on high-speed rail. As the world becomes smaller, we at The Radio Research Group have witnessed firsthand how nearly everything we knew about modern conflict is changing, under the shadow of Fifth Generation Warfare. The incredible, exponential, accelerating pace of technology has overturned centuries of standard operating procedure. Diplomats and military leaders alike have been thrust into uncharted domains, disrupted by an invisible enemy that makes us question our reality.

Darkness descends upon us as a tunnel envelops our train. Terrestrial GSM goes dark, satellite tracking loses sync. We enter the Gotthard Base tunnel, the longest tunnel in the world.

Our world is evolving so quickly that classical frameworks of thought around modern warfare have become irrelevant. Our GSM modem connects to a cell tower deep within the tunnel. We reconnect to the world, deep underground, at the speed of light. Pre-existing notions believed to be impossible beforehand have now become commonplace.

Our train exits the tunnel, sunlight envelops the train as GPS returns back online. Incredible mountains open up all around us as we enter an incredible new world.

What is 5GW?

William Lind's generations of warfare model goes something like this:

Generation	Description	Made Irrelevant By
1st	Ancient melee battle	Muskets
2nd	Organized battle with gunpowder	Blitzkrieg
3rd	Mechanized warfare focused on speed and manoeuvrability	Terrorism
4th	Decentralized warfare is led by state actors (Primarily Kinetic)	The Mobile Internet, Network Effects
5th	*Information and Perception (Primarily Non-Kinetic)*	*TBD?*

The concept of Fifth Generation Warfare itself is controversial, with Lind arguing against it saying that 4GW "had yet to fully materialize". We argue that what is happening in modern conflict today is so radically different from the 4th generation framework that it's time to enter the fifth generation. (We were so convinced that we had to write the Wikipedia article on it ourselves, despite it now being heavily redacted. Many of the key elements we have added here.)

Our favourite definition of Fifth Generation Warfare is featured in Abbot's "Handbook of 5GW", 2010, stating that "The very nature of Fifth Generation Warfare is that it is difficult to define." Besides the fact that defining a subject based on it being difficult to define is counterintuitive, Abbot adds that 5GW is a war of "information and perception".

> 5GW is a war of information and perception.

We at Radio Research have evolved the definition, stating that Fifth Generation Warfare is defined by data-driven, non-kinetic military action designed to take advantage of existing cognitive biases and create new cognitive biases. Or as Abbott and Rees/Herring describe, "the deliberate manipulation of an observer's context in order to achieve a desired outcome."

Fifth-generation warfare technologies have advanced to the point that when applied correctly, their very use has been concealed. As we will describe further below in the Attribution Problem, in many

cases simply understanding who is behind a 5GW attack is impossible.

This means that a Fifth Generation Warfare conflict can be fought and won without a single bullet being fired, or even most of the population knowing that a war is taking place. The following technologies and techniques are often associated with 5GW. What's important to note is that these technologies may be used to heavily influence, or completely remove the need for kinetic combat:

- Misinformation (Data Driven)
  - Deepfakes
- Cyberattacks
  - Honeypots
- Social engineering
- Social media manipulation (Data Driven)
  - Decentralized and highly non attributable psychological warfare (memes, fake news)
- Mass surveillance
  - Open-source intelligence
  - Commercially available Social media analytics
  - Open source and grey market Data Sets
  - Commercially available Satellite / SA imagery
  - Commercially available Electromagnetic intelligence
  - Cryptographic backdoors
- Electronic warfare, with the rapid reduction in cost and availability thereof
  - Open source encryption/ DeFi / Community technology
  - Low cost Radios / SDRs
  - Quantum computers? (unclear if being used yet at scale)

Abbot finished his description of 5GW quite elegantly, quoting Clarke's third law; "any sufficiently advanced technology is indistinguishable from magic."

In Summary 5GW:

- Is a war of information and perception
- Targets existing cognitive biases of individuals and organizations
- Creates new cognitive biases (social engineering)
- Is different from classical warfare for the following reasons:
  - Focuses on the individual observer / decision maker
  - Is difficult or impossible to attribute
  - Nature of the attack is concealed

Below we will describe where current frameworks for warfare begin to unravel, and what we can do next.

Origins

The origins of 5GW as mentioned before are hotly contested, as data driven warfare combined with propaganda date back at least to the end of WWII. Some of the best work in the space happened around this time.

For our analysis, we focus on how networked mobile computing and big data analytics are being used to drive decision making on a societal scale. While the “Handbook of 5GW” alludes to early examples, the book was published before one of the most disruptive societal events had happened since 9/11.

Egyptian protestors shine high powered lasers at a helicopter, disrupting its optics. (Source)

Precursors to 5GW: The First Accidental Fifth Generation Conflict

The Arab Spring represents a key turning point in warfare, emerging in Tunisia in 2008, and erupting across North Africa in 2010. The Arab Spring was the first conflict to be driven by Social Media, primarily Facebook and Twitter.

We had witnessed first-hand that a revolution or protest would show up first in the data, then on BBC a few hours later. The conflict was manifesting itself online, and generating tremendous amounts of data before any kinetic action would take place.

The Arab Spring lacks a few key elements of Fifth Generation Warfare, most notably the ambiguity of the opposing force. (Despite having some ambiguity as to who was fueling it. An interesting side note is that one of the main organizers of the Egyptian Revolution, Wael Ghonim, worked at Google at the time).

From our interactions with people involved during those early years of mostly privatized data collection, the use of social media to cascade into a regional conflict was almost entirely accidental. Because of that, we like to call The Arab Spring the first accidental fifth-generation conflict.

The societal echoes of the Arab spring continued to bounce around the planet, focusing a few years later on Hong Kong and Taiwan during democratic protests in 2014. At this point, we begin to see a new technology beginning to emerge: Decentralized technologies (or “zero trust systems” for those of you who work in more conservative organizations like the DoD). During the Sep 2014 Hong Kong protests, encrypted messaging apps were used heavily. When local cellular infrastructure was “overloaded” protesters employed a decentralized Mesh networking app called Firechat- completely bypassing Great Firewall restrictions. Governments were so disturbed by the event, Russia began deploying its own electronic warfare units to protests.

Decentralized currencies like Bitcoin began to see popular use, For example during Occupy Wall Street, 2011). While decentralized warfare is a key element of the 4GW definition, the coming ambiguity of attackers and the use of big data and media as a weapon reinforcing one another takes us into new realms.

Fitting a Fifth Generation Warfare puzzle piece into a Fourth generation playing field

While warfare has a long history of psychological operations and propaganda, conflict going online has accelerated psychological warfare, reducing the feedback loops to milliseconds. Facebook product teams have a word for this: “Dopamine Loops”. In the world of big tech, you can build, test, deploy in a matter of minutes. Military, advertising, and political strategists are beginning to think about how they can leverage over a hundred years of teachings in psychological warfare and combine this knowledge with data-driven, psychological feedback loops to influence behaviour.

We call this the Social Engine, Facebook (sorry “Meta”) calls it “business as usual”. The creation of data-driven cognitive biases has already defined the past decade, everything from “swinging” elections, to determining a Netflix script, or which celebrity will be in an advertisement for makeup.

In fact, we used GPT-3, an AI algorithm to write the italicized section of this paragraph. *GPT-3 is a predictive text entry program, which allows people to type words on their keyboard by predicting keys that are likely to be typed. This allows us to influence cognitive biases by sneaking certain ideas into peoples' text, bypassing their critical thought processes altogether. People will then replicate these messages in their own texts, and the spread of the content will be a reflection of the users' natural cognitive biases.*

These capabilities are unseen in traditional warfare and do not fit well into the 4GW framework.

One of the main areas where 4th generation warfare begins to break down is the ambiguity of the attacking force, in particular, "the cyber attribution problem". This is related to the fact that software engineers are actively hiding or misconstruing their identity while writing lines of code. In some cases, hackers are even using modified cyberweapons leaked from NSA servers (see EternalBlue, 2017).

In a Fifth Generation of cyberwar, simply knowing who your enemy is can be nearly impossible.

The Attribution Problem

The cyber attribution problem has highlighted the problems of traditional warfare, as almost all modern military doctrine requires knowing the identity of your enemy. This is where modern conflict begins to get outright frightening. Governments have routinely stated that cyberattacks can and will be responded to with kinetic force.

In the 2018 edition of the "U.S. Dept. of Defense Nuclear Posture Review" the U.S. government states that they reserve the right to respond to "non-nuclear strategic attacks" with "the employment of nuclear weapons". The fatal flaw of nuclear deterrence is that it does not apply only to nuclear weapons.

"The United States would only consider the employment of nuclear weapons in extreme circumstances to defend the vital interests of the United States, its allies, and partners. Extreme circumstances could **include significant non-nuclear strategic attacks**." (Insert Citation)

The Nuclear Posture Review itself mentions "Cyber" sixteen times. Considering some of the largest cyberattacks in history was started by teenagers, (Mirai botnet, 2016) the impact of The Cyber Attribution Problem on modern nuclear deterrent theory is quite literally insane.

"We used to be able to get into a room with an enemy, now they're just floating in the ether,"
-M speaking to Bond in No Time to Die, 2021

A new era begins.

The Birth of Fifth Generation Warfare

Social media in its essence (along with most of the internet today) is driven by for-profit cognitive programming, also known as advertising. Ads along with the exponentially growing set of "Advertising" data generated by billions

of people have now been weaponized. The amount of data that can be collected on an individual is increasing exponentially.

We argue that the first compelling case of Fifth Generation Warfare was the 2016 U.S. Presidential Election. This includes complete ambiguity of the opposing force, wide-scale societal engineering using data (see Cambridge Analytica), organized counterattacks between government and social media companies, censorship, and the direct attack on the decision making process of billions of people.

We encourage you to read the leaked internal Facebook report detailing precisely how this is taking place from the perspective of a computer scientist. It's fascinating and very scary: "Stop the Steal and Patriot Party: The Growth and Mitigation of an Adversarial Harmful Movement").

Unfortunately, the 2016 presidential election gets too political for most readers, as their own cognitive biases prevent the creation of a subjective Fifth Generation Warfare framework. We may update this section in the future, and continue our story of 5GW with something far less controversial.

Israel, May 2021: Operation Guardian of the Walls

The Israeli Defense Forces (IDF) are masters of information warfare. Israel even has their own propaganda division of the military, the IDF Spokesperson Unit. They have a pretty cool logo, representing the propagation of radio waves.

The first 5GW conflict to evolve into a kinetic battle (excluding the storming of the U.S. Capitol a few months before) took place during the 2021 Israel–Palestine conflict. On May 13th, 2021, the IDF announced falsely on Twitter, and on the record to The Wall Street Journal, that "IDF air and ground troops are currently attacking in the Gaza Strip". The IDF had announced that an Israeli invasion of Gaza had begun.

The New York Times then reported the following day that the announcement had been a deception, that no Israeli troops had stepped foot into Gaza. IDF further clarified the statement declaring that the intent of the announcement was to expose opposing Hamas forces (presumably using unmanned ISR) and destroy tunnel networks with precision-guided munitions.

Katz and Bohbot describe separately in their book "Weapon Wizards, 2017", how IMSI-catchers and cellular network analysis were used to previously identify and destroy Hamas tunnels. If an IMSI "teleports" from one place to another, it's a tunnel. A single fighter (likely many) forgetting to turn off their cellular transmitters after the news reports may have resulted in massive, heavy bombing attacks. There is so much data in our corner of the universe, that the absence of data can even provide information.

The IDF Spokesperson's Unit announced two weeks after operation "Guardian of The Walls", that the conflict was the "First AI war". IDF continued to describe a system built by Unit 8200 that fused "signal intelligence (SIGINT), visual intelligence (VISINT), human intelligence (HUMINT), geographical intelligence (GEOINT)". While such battlefield management systems (BMS, or C5ISR) have existed for years before the 2021 Gaza crisis, the announcements themselves combined with social media deception and precision-guided munitions represent a stark contrast to the Lind definition of fourth-generation warfare.

The IDF example does however lack “ambiguity of the opposing force”, but does include many unprecedented techniques and technologies- most notably using media as a weapon combined with unmanned ISR.

From here take a quick coffee break, before we dive even deeper into the strange, mind-bending and brain-frying world of Fifth Generation Warfare.

A Syndrome in Havana: A Symptom of Fifth Generation Warfare?

Our last example, Havana Syndrome, includes the purest form of Fifth Generation Warfare we have witnessed to date. It is also one of the weirdest. Havana Syndrome checks all of the 5GW boxes:

- Ambiguity of the opposing force.
- Ambiguity of attack vector.
- Dopamine loops.
- Triggering existing cognitive biases in target.
- Creating new cognitive biases.

In fact, Havana Syndrome is so obscure there is significant debate within the U.S. DoD on whether or not it even exists.

Havana Syndrome was first reported in and around the Cuban embassy in 2016 and has since been reported all around the world including Guangzhou, Hanoi, Berlin, and most notably Vienna, Austria.

Diplomats report hearing strange noises and headaches, resulting in significant neurological damage. The US Army Mad Science Lab interviewed Dr James Giordano, one of the doctors involved in researching the cases.

You should read the deleted report, it is extremely interesting: (Link to report)

As Dr James Giordano describes to the U.S. Army Mad Science Lab:

> “To date, there are over 100 validated cases of personnel being afflicted with the subjective symptoms and clinically validated objective signs representative of Havana syndrome…
>
> “ The acute symptoms are relatively ambiguous, in that some individuals report sensations of pressure in the head, ringing or buzzing in the ears, and feelings of confusion…
>
> “The majority of the originally affected individuals, and many of those subsequently affected have shown long-lasting, discernible neurological features that are evident upon physiologic testing and imaging…”.

To make things even more interesting, the State Department recently declared that 5GW was no attack at all, simply a cricket, *Anurogryllus Celerinictus*, and that psychogenic effects were the primary cause of reported health issues.

The Army report has since been deleted. *We do love 5GW!*

The last we checked, there is no *Anurogryllus Celerinictus* in Vienna or Berlin, but go read the DoD report for yourself. The very nature of the attack being ambiguous, and the heated debates between DoD and even CIA officials over causes and existence make “Havana Syndrome” fit perfectly into our 5GW framework.

Take a look at the DoD report on crickets: (Source)

We surely have not seen the last of our friend *Anurogryllus Celerinictus*, and expect to see more attacks like this play out in the future. *(We think it is a Massive MIMO attack using modded cell towers, but that’s story for another day)*

History of Fifth Generation Warfare Summary:

5GW Checklist:

- Ambiguity of the opposing force.
- Ambiguity of attack vector.
- Dopamine loops.
- Triggering existing cognitive biases in target.
- Creating new cognitive biases.

- Emerges from The Arab Spring.
- Solidified during the 2016 U.S. presidential election.
- The 2021 Israeli-Palestinian conflict was the first example of 5GW in kinetic battle.
- Havana Syndrome is pure 5GW.

From here, the future is incredibly uncertain. We lie at the brink of WWIII in Europe. Deep Fakes are being created by both sides. It is more important now than ever to begin thinking about 5GW. We have attempted to organize a *framework of thought*.

Our thinking on this is evolving rapidly, as cognitive bias plays a role in influencing each section of the OODA loop. Here are some recommendations:

Observe: What’s happening. Understand the battlespace, attempt to single out the opponent or describe key attributes. Get as much data as you can and hire the best people who can work with that data. China is doing this by building a network of “AI consultancies” around the earth, along with backdooring apps for kids to feed massive amounts of data back to Beijing. The U.S. does this by working with Facebook, ISPs, and controlling Android. Hedge funds have a lot of this data as well. Maintain caution when developing your own mass surveillance tools, as this may accelerate the systemic issues in your society, and the enemy will target these weak points within your own team. Mass surveillance generally poses more risks to civilization than benefits. Is mass surveillance a deterrent technology? This is open for debate and becomes increasingly relevant in 5GW.

Orient: Attempt to understand any pre-existing cultural biases you may have. 5GW attacks the decision-making ability using the biases as cognitive tools of influence. What memes do you like or political groups you do prefer, what are your fetishes and dislikes? What skeletons do you have in the closet? How do you use social media? How’s your relationship going with a loved one? All of this data is being harvested from your internet history and the

spatial web and will be used against you in a world of Fifth Gen targeted warfare. (Most of this data is commercially available on the grey market).

Once you establish a psychological baseline, we can try to separate cultural biases from cognitive biases. A meme you viewed the day before can certainly impact decisions you are going to make today. The only recommendation we have here so far is to reduce your digital attack surface, go spend time in nature, and meditate. Meditate on your pre-existing cultural biases to build a baseline and understand where your ego will play in your subconscious decision-making processes. Humans really haven't progressed very far in understanding this front, and some of the best work on this is thousands of years old. We recommend starting with the Bhagavad Gita.

Decide: We now have to choose the best strategy to recover faster, move forward, and act with minimal damage. See if you can test your hypotheses, and watch out for making the same decision over and over again. In many cases, you simply have to "move fast and break things", and make sure that when you do Act that you get data. Have the means to analyze this data at scale and a plan for a complete breakdown in communications. Ideally, you have some insanely large supercomputers to help you, the latest Facebook Graph, and that you watch out for biases in your own algorithms. In many cases the Fractional Orbital Bombardment System will already be orbiting, your servers will be on fire, your comms backdoored, and you won't have the pleasure of testing your theories.

Act: Pull the trigger, and get as much possible data as you can in the aftermath. In the end, we're all human, this is what will be used against us.

We Are only at The Beginning of 5GW

Hopefully, we could give you a quick overview of what the hell 5GW is, its history, and how we can begin thinking about it. Our definition of a 5GW framework is evolving, and we encourage you to contribute to the conversation and challenge our thinking.

Denying that 5GW exists is incredibly dangerous, and we see a tremendous divide between the hackers and cryptographers we speak to and officials in the public sector. Most people we speak to at the DoD think we're completely crazy.

The attacks that we will begin to see will quickly evolve beyond "crickets" and into the bizarre and seemingly impossible. It's easy to get rather depressed about a future of biological and nuclear deterrence, massive social engineering attacks, and hypersonic proliferation concerns. **But we must always remain positive.**

Thinking about the world in regards to limited resources, (a war of "us" vs. "them") is the root of much of the world's issues. Our economy is moving digital, and incredible technologies are coming online that solve most of the resource-driven conflicts that we have seen historically:

- Petrochemical – Nuclear
- Drought – Desalination
- PetroDollar – DeFi
- Disease – mRNA/ CRISPR
- Advertising – Web3

Civilization requires a fundamental shift in our organizations and institutions towards a perspective of abundance, with a strong focus on defence based deterrence (e.g. password managers or the Iron Dome). Data is going to help us. Understanding and mastering 5GW is going to be key.

And to finish, we once asked a DARPA program manager how they stay optimistic about the future, having witnessed so many technologies that could wipe civilization off the face of this earth. The ex-program manager responded, “Civilization has been through a lot, they always get through!”

The future is going to be incredibly interesting, and we’re excited to see it.

5GW Recommendations:

- Use the OODA loop to build a framework of thinking.
- **Defensive:**
  - Understand basic cybersecurity: Use a password manager and hardware security keys. Understand your own biases, culture and those that have inflicted you (media, memes)
  - Meditate and understand your own biases
  - Map your electronic attack surface and Work to limit your digital footprint (e.g. who has access to your location data?)
  - Attain complete technology awareness on your domain
  - Map and visualize filter bubbles
  - Assume your entire network is going to get attacked, taken offline and have a plan
  - Do not underestimate blockchain, learn about zero knowledge proofs and DAOs. Read the Blockchain And Decentralized Systems by Pavel Kravchenko for everything you need to know technically. Read The Sovereign Individual for a good understanding on the societal implications.
  - Assume all commercial cryptography is either backdoored or will be broken during the next great conflict
  - Map your cryptographic roots or trust and have a key management plant
  - Invest in modern communications equipment and “zero trust systems”
  - Pay for security audits and Red teams if you are an organisation
  - Red team your systems.
  - Red team your people, perform simulated phishing exercises.
- **Offensive:**
  - 5GW is mostly defensive, but there are a few things to be done.
  - Inoculation Theory. A fairly new concept for resisting social engineering, but a focus on reinforcing an idea by presenting the intended target with weak counterarguments. A recommendation from Over The Horizon: (Link)
  - Surveillance, Controversial but effective, at least in understanding a baseline.
  - Censorship. Social media companies are a business of influencing cognitive bias.
  - Generation of fake and alternative profiles and data, hide in the randomness. See Sybil attack, sock puppet accounts.
  - Meme warfare.

    - Make social media algorithms accountable and open. This is a major problem today as social media reinforces cognitive biases, generally for profit.

Essential reading on the history and future of propaganda, and information warfare:

- Massenpsychologie (Group Psychology and the Analysis of the Ego), Sigmund Freud, 1921.
- Propaganda, Edward Bernays, 1928 (heavily inspired Propaganda Minister Goebbels).
- The Ultra Secret, F.W. Winterbotham, 1974. The first “tech leak”, the book goes into detail in the breaking of the Enigma Codes at Bletchley Park, along with the propaganda campaigns organized by Churchill and Special Liaison Officers to hide Ultra’s use.
- Berlin Diary William L. Shirer, 1941. Describes the compelling account of WWII breaking out in Europe as it’s happening, as described by a CBS news correspondent. His descriptions of Nazi propaganda and arguments with censors is fascinating.
- Black Swan, Nassim Nicholas Taleb, 2007. Just read it.
- Snow Crash Neal Stephenson, 1992. (Science Fiction) An extremely entertaining account on information warfare, literally defined the “MetaVerse” and “Avatar”