Dear Reader,

This is an excerpt of something discovered by one of our members. It has a number of valuable concepts we could apply to our cause.

Let’s keep these cards close to our chest.

-O

> *“Can you not see it brother? The rainbow bridge to the superman?”*
>
> *-Nietzsche*

> *“Man is a bridge between ape and superman, a bridge over an abyss.”*
>
> *-Nietzsche*

> *“The mastery of nature will be accomplished through number and measure.”*
>
> *-The Angel which appeared to Descartes;*
> *instructing him to pursue the scientific method.*

THE NETWAR MEMO

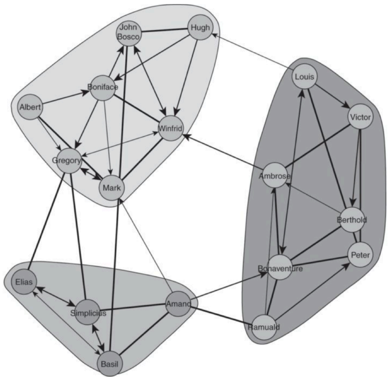
1.0 THE GLOBAL BATTLE SPACE

Netwar is war against the entire network of relationships, culture, values, information, resources, and infrastructure of an enemy. The netwar model views societies as massive networks extended across domains, and frames geopolitics as conflict between these networks. Through this lens, chains of causality—extended globally via networks of relationships—constitute the battle space of modern geopolitical conflict. Nothing occurs in isolation. Everything is part of the global netwar.

Networks are composed of two primary features: individuals and their connections. The individual is referred to as an **actor** and their connections are referred to as **ties**. Actors can be individuals or represent larger organizations, such as Department of Homeland Security or Disney. Ties are connections between actors which serve as conduits for the diffusion of goods. These goods can be things such as resources or information. Ties can vary in strength and have elements of directionality, where goods flow in one direction more than the other, such as the flow of information from a news outlet to viewers. Ties with directionality are referred to as **arcs.**

Networks differ in the organization of their structural elements, which is referred to as **network topology.** Networks have different levels of **density** and **fragmentation.** Density and fragmentation describe the overall structure of ties between actors. Gaps created by fragmentation are referred to as structural holes, and actors who bridge them are referred to as brokers. The network of the Sampson monastery is displayed below:

Fig 1:



I. ACTORS: the units of a network. These can be individuals in an organization, companies in a supply chain, or neurons in the human brain. These are represented by circles in *fig-1*.

II. TIES: the connections between actors. These can be roads, fiberoptic cables, or conversations. They serve as conduits for flows of goods. Goods are things like copper, energy, people, or information. These are represented by the lines connecting the actors in *fig-1*.

III. ARCS: are ties with an element of directionality. These are connections like those between individuals and television networks, where flows go more in one direction than the other. Arcs describe the ties in the chain of command, and communication between superiors and subordinates in a business. These are represented with arrows in *fig-1*.

IV. TIE STRENGTH: the amount of goods that flow through a given tie. For example, the difference between an eight lane superhighway and a country road; or between 3g and 5g. The strength of a given tie is represented by the thickness of the line in *fig-1*.

V. NETWORK TOPOLOGY: descriptions of patterns of connection.

VI. DENSITY: describes how interconnected the actors in a region of a network are. Members of the software department at Apple will have a higher density of connections to each other than they have with members of the hardware or marketing departments. This same pattern of differential densities holds true for sports teams, nations, and families. Areas of high density are outlined in grey in and represent different factions within the monastery in *fig-1*.

VII. STRUCTURAL HOLES: describe a lack of connection between dense regions. These are the gaps between departments in an organization and the space between the two hemispheres of the human brain. These are the non-grey regions between the three areas of high density in *fig-1.*

VIII. BROKERS: are actors whose ties bridge structural holes. Between states, diplomats can the role of brokers. In the global economy middle men create value by serving this role. Gregory and Elias are brokers between their respective regions of high density in *fig-1*.

IX. BRIDGES: The ties between brokers. These can be things like bridges across a rivers, maritime straits, a undersea fiber optic cable, or a cell signal.

The battle space in which the global netwar is fought can be conceptualized as structurally composed of these basic elements. As an example, the trade war with China is fragmenting the global economic network. Tariffs forced companies to reduce ties to China, creating structural holes between the network of Chinese suppliers and U.S. consumers. As companies moved their manufacturing out of China to places like Vietnam, they became brokers between the Vietnamese economic network and the U.S. network. The bridges between these two networks then serve as conduits for goods, capital, and information. As ties increase across all these domains, the network density of the trans-Pacific network will increase, which could challenge the hegemony of China in Asia.

The annexation of Crimea can be described in these terms as well. Russia created structural holes between Crimea and Ukraine while creating a number of bridges between Crimea and Russia's Eurasian network. This operation was ongoing long before Russian Special Forces showed up in Sevastopol, slowly altering the network topology of the region in Russia's favor.

The 'Crimea operation' was the final reorganization of a network which had been being prepared for reorganization for some time. To accomplish this, Russia disrupted Western networks with information operations as it also activated a number of assets to rapidly alter regional network topology. Russian Special Forces physically disconnected the internet hubs which created bridges between the information environments of Crimea and the West, creating a large structural hole**.** Simultaneously, Russia began increasing network density between itself and Crimea by handing out Russian passports, promising free healthcare, and eventually building a physical bridge between the Crimean peninsula and mainland Russia.

These ties, across multiple networks, all served the same geopolitical purpose and are brought into focus with the network geopolitics model. The application of this model to the examples above demonstrates the utility network geopolitics has for interpreting global geopolitical dynamics, and provides the context for understanding the effects of information warfare in the cyber realm on these global networks.

The Crimean operation and ongoing European netwar also have very strong cyber components. During the Crimean operation, Russia carried out a number of disruption campaigns via social media. Afterwards, these disruption campaigns evolved into targeted operations to alter the network topologies of the United States and its NATO allies. Russia's primary focus was on continuing to widen structural holes through operations against brokers in the West.

During a NATO patrol through Eastern Europe, several U.S. soldiers were accused by name on Russian news outlets of child rape. These stories were then distributed virally on social media. No evidence was ever presented for these claims, but these Psychological Operations (PsyOps) were designed to take advantage of U.S. cultural norms which vilify those accused of certain crimes regardless of evidence of guilt. This threat of reputation destruction was an attack against the network of security relationships between NATO, the United States, and Eastern Europe—and highlights the multi-domain quality of netwar operations. This PsyOp against U.S. servicemen intersected the cyber domain in pursuit of goals which extended beyond it. This is the common character of netwar operations and must be kept in mind when creating effective policies. While disciplines like social cybersecurity are focused on challenges in the cyber realm, the network with which it interacts extends far beyond it.

Information operations effect the topology of ties and arcs which serve as conduits for a number of goods. Operations against the informational network can effect the flow of non-informational networks such as natural gas, grain, arms, and manufactured products. An ongoing debate in regard to Ukraine is whether to establish ties which would serve as conduits for lethal military aid. This debate is occurring through flows of information exchanged between actors within the decision bodies of the U.S. government—but the effects were on the topology of non-informational networks.

The network of global supply chains which transforms raw materials into an iPhone is organized by information networks as well. The same holds true for the networks which transform opium poppies in Afghanistan into a ten euro bag of heroin in Portugal, with an accompanying syringe manufactured in China. This dependence of all other networks on informational networks for their organization is a key feature of network geopolitics and brings into focus the importance of information warfare in the global netwar.

Information warfare takes place in a network whose ties serve as conduits for information. This informational network connects the minds of individuals to their communities and is the medium through which culture is transmitted, updated, and stored. This network organizes human groups by directing their collective behavior. The collective behavior of groups is what creates and maintains global networks, and consequently the information network's ability to organize the collective behavior of individuals makes it the strategic high ground in the global netwar. Information warfare is the battle for this high ground.

2.0 INFORMATION WARFARE

Information warfare affects global network topology by targeting the cultural information which organizes group behavior. The battle space of information warfare is the network of ties between individuals which serve as conduits for '**memes.**'

Richard Dawkins described memes as units of cultural information analogous to the gene in biology. The American eagle, the jingle from a McDonald's commercial, and the memory of the Coca-Cola logo are examples of memes. John Gottsch, Paul Marsden, Derek Gatherer, and Michael Best have separately described how memes diffuse across interpersonal networks in sets as **narratives,** and how memes have the ability to change group values and behavior. Human groups are networks of ties which act as an environment in which memes interact and compete. These memes form narratives which become the culture that directs collective behavior. Collective group behavior organizes all aspects of the global network. This makes information warfare's ability to affect group behavior a key element in the global netwar.

The fundamental unit of information warfare is the meme. Memes exist as a network of associations which extend across internal and external space. Internal memes (**i-memes**) are things like a tune which gets stuck in your head, the memory of a your childhood pet, or the subjective feeling you get in response to an external stimulus. External memes (**e-memes**) are **i-memes** which have manifested in the environment as behaviors or **artifacts.**

Artifacts are objects which have memetic signal value like the American flag or the Christian crucifix. Behaviors and artifacts serve as stimuli for i-memes creating a feedback loop which directs collective group behavior. The meme of 'patriotism' extends across a number of internal and external representations. These can include memes in the form of visual and auditory memories, and the feeling one gets when seeing the American flag. The flag is an artifact of the meme of patriotism and helps maintain a feedback loop with i-memes which direct the behavior of patriotic Americans. The meme of patriotism can also be expressed through behaviors, such as posting an e-meme to social media, laying a wreath at the World War II memorial, or saying the pledge of allegiance. The totality of this network of associations and behaviors constitutes the meme of 'patriotism'.

The Defense Advanced Research Projects Agency (DARPA) has funded numerous projects dedicated to **military memetics** in recent years. These projects have included studies of ideas as contagious entities analogous to diseases, the use of these ideas in military operations, and information networks as narrative environments to spread memes. DARPA analyzes the effectiveness of memes based on their **propagation**, **impact**, and **persistence**:

- **Propagation** is a meme's ability to spread between individuals with dynamics resembling a biological weapon, described with terms such as virility and "vectors of infection".

- **Impact** is the extent to which a meme modifies an individual's beliefs, values, and behavior.

- **Persistence** is a meme's ability to survive within a host for a long period of time, extending its window of propagation and impact.

In 1962, a narrative about a "June Bug" whose bite would cause numbness, nausea, dizziness, and vomiting swept through the information network of a U.S. textile factory. This narrative caused 62 workers to report symptoms. No bug has ever been discovered which creates these symptoms and none of the workers demonstrated bites. The U.S. Public Health Service's Communicable Disease Center was called in to investigate and concluded the 'June Bug Incident' was caused by mass hysteria. The memes which caused this hysteria had a high level of impact, causing psychosomatic illness in the individuals it inhabited. They were highly contagious within the dressmaking department of the textile factory, but did not spread beyond it, demonstrating interesting propagation dynamics. These memes only lasted for a few days, indicating weak persistence. Other memes and narratives last much longer.

The memes which made up narratives of communism were some of the most potent memes in history. They had enough impact to motivate their hosts to overthrow numerous governments and propagated broadly following the Bolshevik Revolution. They have demonstrated an incredible ability to persist despite the incredible global death toll for which they are responsible. In U.S. universities, 18% of social science teachers still identify as Marxists. The artifact of the hammer and sickle is fashionable on college campuses among the students to which these memes have propagated via the ties between students and faculty maintained by the university system.

The artifact of the swastika has not had the same level of persistence, despite having high levels of propagation and impact. While National Socialism in Germany was responsible for six million deaths with its final solution, communist memes have been responsible for over 60 million deaths in China and 20 million deaths in Russia alone. The persistence of communism has to do with the structure of its network of associations. Nazism is linked inextricably with a network of e-memes and i-memes which generate feelings of horror. Communism has persisted because of a set of e-memes responses—that none of '*that*' was really communism. Asking someone who claims to be a Marxist about the death tolls in China and Russia will generate the same behavioral response across cultures and geographic regions. Marxists will claim that neither of those examples were really communism, that Stalin and Mao's versions were aberrations of the pure Marxism, which will bring about utopia. This shows a consistency in behavioral coordination across groups which speaks to the power of memes to direct collective group behavior. These dynamics are what information warfare seeks to utilize in order to alter network topology.

Information warfare's role in the global netwar is to affect the behavioral organization of geopolitical networks by attacking narratives with memetic weapons.Narratives are composed of sets of memes which organize group behavior over time. They bind individuals into communities, determine collective goals, and organize group behavior in pursuit of these goals. By distorting and amplifying specific memes within groups narratives, memetic weapons can alter the behavior of that group.

Several recent U.S. Senate reports have outlined the use of memetic weapons against U.S. citizens. These weapons caused domestic groups to behave in ways which supported our enemies and were part of wide sweeping information operations carried out via social media. These information operations are perfect examples of what social cybersecurity must address. In the modern information battle space, the ties which serve as conduits for memetic weapons are primarily facilitated by social media platforms.

3.0 SOCIAL MEDIA BATTLE SPACE

The memes transmitted through social media have been used in the global netwar to annex territory, inspire terrorist attacks, and overthrow governments. Social media is a subdomain of the network which makes up the broader internet, however, it is also the primary mechanism that helps people decide which of the 1.5 billion available websites to create ties with. The network of ties maintained through social media is the primary battle space in which the modern netwar takes place.

The social media battle space is a very simple environment. On a mobile device, social media is a series of e-memes arranged vertically in an **infinite scroll.** These e-memes can be cute cat videos or memetic weapons. The user's responses to e-memes are monitored by social media platforms and used to fine-tune the infinite scroll with deep learning algorithms. As these algorithms adapt to user preferences, social media becomes so engaging that use of the platform begins to resemble substance addiction.

Nir Eyal and Ryan Hoover have outlined how social media addiction has been consciously engineered into platforms by software engineers. Social media's profit model is based on winning the battle for attention against all other stimuli in a user's life. This is done first with external triggers like notifications, and then engineered to become attached to internal triggers like boredom or loneliness. Platform engineers accomplish this by targeting specific neurotransmitter systems. These are the same systems implicated in methamphetamine, cocaine, and opioid addiction. Social media has perfected its use of these mechanisms for behavior modification to the point that many of the software engineers that created these platforms have stopped using smart phones.

In addition to creating addictive engagement, social media platforms collect data on users to alter their behavior on behalf of paying customers. This data is used to determine the personality, preferences, and psychological vulnerabilities of users to specific behavior modification techniques. Women's mensural cycles are tracked for this purpose using alterations in gait measured by the accelerometer, as are cyclical mental health conditions such as bipolar disease. Data is also used to fine-tune behavior modification for specific personality types. This data is intended for use by companies to modify the economic behavior of users with advertising. It is also used in the global netwar for targeting and tuning memetic weapons for propagation, persistence, and impact.

This battle front in the global netwar gives fine-tuned memetic weapons access to large portions of the global population. Worldwide, people spend an average of two hours and sixteen minutes per day on social media. This ranges from a high of four hours and 12 minutes in the Philippines, to a low of 36 minutes in Japan.

The primary social media platforms used worldwide are Facebook, YouTube, Instagram, Twitter, and WeChat. These corporations have a fiduciary responsibility to their stockholders which mandates their primary focus be on maximizing profits. Consequently they keep staff to a minimum. Twitter has 4,600 employees while the platform generates 500 million tweets per day (350,000 tweets per minute), with some regions tweeting in languages no one at Twitter can understand.This staff/content ratio is similar at the other social media platforms and leaves this battle space largely unregulated, making it an ideal environment for large scale information warfare through memetic weapons.

This lack of regulation, coupled with addictive user engagement and global penetration, has made social media a primary battlefront in the global netwar. It gives adversaries direct access to the information networks which organize all other global networks. This brings into stark focus the enormity of the problem the United States has to address. Beyond the defense of domestic narratives, it must defend the narratives which organize the global networks on which the U.S. standard of living is based. Every person with a smart phone carries the global netwar in their pocket and is providing a constant stream of data which can be used to fine-tune the memetic weapons targeted at them. The vast majority of actors are completely unaware of the battle space they enter multiple times per day—and the memetic weapons which target them on a daily basis.

4.0 THE PLAYERS

The primary actors in the social media battle space are individuals, **trolls**, **bots**, and **dupes**. The term 'individual' is used to describe an average person on social media. In this section we discuss how individuals interface with the environment to create attack vectors for memetic weapons and the process these weapons use to take control of behavior. After outlining this process we discuss how different types of trolls and bots facilitate this process. Finally, we briefly discuss dupes, individuals whose behavior has been successfully co-opted by memetic weapons

4.1 THE INDIVIDUAL

The bulk of actors whose ties make up the social media network are unaware of geopolitics or the netwar. These individuals know very little first hand about the world and have acquired most of the memes which make up their narratives from authority figures and media. They use social media to signal their tribal affiliations to these narratives and exchange memes related to them as part of their instinctual need to socialize. The memescape this instinctual socialization puts on display provides a rich target environment for memetic weapons.

Memetic weapons use e-memes on social media to modify the behavior of individuals through the feedback loop between their nervous system and the environment. In the global netwar our enemies use this process to alter network topology. The human nervous system takes in perceptual information from the environment, processes it, then produces behavioral outputs. Norbert Wiener described this process as forming a loop and Larry Swanson's model of the nervous system has made this loop model the basis of functional neuroanatomy. At each iteration of the loop the behavioral output impacts the environment, creating new perceptual inputs. Over time the individual calibrates the effects of their behavior on the environment by self-directed behavior modification. These modifications are the result of physiological changes in the neuronal assemblages which process perceptions. By hijacking this natural process of behavioral calibration our enemies can create behavioral outputs which alter network topology to their own ends.

When learning to drive a car, the perception of the road becomes internally represented via the transformation of the environment into neuronal impulses. These impulses are transformed through processing into behavioral outputs such as hitting the breaks or changing lanes. When first learning to drive a car we have to remember to check blindspots and signal before merging. As we go through multiple iterations of the loop, neuronal assemblies take control from our conscious mind and these behaviors become automated. The perception of a slow truck in our lane seamlessly becomes a complex behavioral output consisting of checking mirrors, calculating the speed of all other cars in our vicinity, a change of acceleration to match traffic, signaling with a blinker, and turning the wheel to merge. Swanson described how this behavioral output is calibrated over time through physiological changes in the neuronal assemblages which transform perceptions into behavior—storing patterns from the environment as interaction habits. Players in the global netwar take control of these interaction habits to influence network topologies.

As we engage in a habituated behavior this loop is ongoing. This allows behavioral outputs to be modified by modifying the environment. George Miller, Eugene Galanter, and Karl Pribram described this process, which has become a cornerstone of modern psychology and artificial intelligence.

If the wind conditions change while we pass the truck, the perception of this becomes a new input into the system. Based on this real-time feedback, we will adjust the steering wheel to compensate for the wind. An active feedback process is clearly evident in a slide on ice. As the car begins to slide you remove your foot from the accelerator and steer in the direction you want to go. If the car begins to slide in another direction this new feedback produces a new behavioral output which returns the car to the desired path. In inexperienced drivers this loop can become unstable as uncalibrated processing produces problematic behavioral outputs. Inexperienced drivers perceive the slide, panic, and whip the steering wheel in the opposite direction. This behavioral output then causes a more extreme slide in the other direction which becomes a new input. This new input causes an equally more extreme behavioral response, which becomes the next input.

This process continues as a **feedforward loop**—with each iteration becoming more and more extreme—until something external to the system intervenes in this process: a tree, a snowbank, or an oncoming car. This experience can result in learning, which alters neuronal assemblies and subsequent behavioral outputs for future slides.

Neuronal assemblies are continuously calibrating the transformation of perception into behavior in this way, fine tuning human behavioral responses to the environment. Positive stimuli encourage more of a given behavior, while negative stimuli will reduce a given behavior. Players in the global netwar can use memes on social media to create feedforward effects, influence learning, and deliver positive and negative stimuli. In this way they can influence the behavior of individuals beyond the platform.

When individuals exchange memes via social media, they transform e-memes into i-memes, processes them, then produce new e-memes.

Their social network provides feedback on these e-memes and this feedback helps calibrate the future transformation of memes by rewiring neuronal assemblies. Individuals learn what sorts of posts (e-memes) receive the most positive feedback and adjust their outputs to receive more of this positive stimulus.

In this way, the global information network extends from the environment into individuals' nervous systems. In face-to-face interactions individuals receive feedback through a number of channels including body language, voice tone, implications, and interruptions. On social media individuals adjust their memetic outputs based on a much smaller set of feedback channels such as 'likes' and the memetic content of text responses.

These feedback channels contain much less nuance than those in face-to-face interactions and may be creating feedforward loops which distort U.S. culture as a consequence.

Each actor in the global information network can be conceptualized as one of these loops—constantly engaged in memetic processing of U.S. American culture by taking in and producing memes which collectively make up the U.S. memeplex. In this way the global information network extends into individual's internal network of associations and habituated responses.

The entire system is susceptible to runaway feedforward processes which have seen in events like the Arab Spring. Social media maintains a massive network of these processing loops through ties not limited by geography. This massive increase in interconnectivity has made the entire global information environment more susceptible to information warfare. Memetic weapons are engineered to operate in this landscape of loops for propagation, persistence, and impact—altering the behavior of individuals.

The e-memes received through social media can produce behavioral modifications which extend beyond social media platforms to global geopolitical networks. These behaviors have led to genocide, terrorist attacks, and coups. Some of these large scale memetic behavioral modification events emerged through the self-organizing feedforward dynamics of the social media environment.Others were engineered by intelligence agencies as part of the global netwar.

The process of behavioral modification consists of the three stages of perception, processing, and behavioral modification. Memetic weapons use this three-stage progression to alter the physiological structure of their target's neuronal assemblies, and eventually their behavior beyond the platform. Behavioral modification operations take place over many weeks, months, or years. During this time, individuals are exposed to multiple memetic weapons and moved into progressively more isolated information networks. These memetic weapons both alter the structure of the internal information network, and the structure of the social network on which the individual is embedded.

Establishing control over individuals with memetic weapons via social media is a three phase process of behavioral modification. This process prepares people for isolation by taking control of their perceptions, isolates them, then transforms their behavioral outputs:

- **Phase 1:** Alter the targets i-meme responses to e-memes.
- **Phase 2:** Isolate the target from other memetic influences, reducing the competition for their behavior.
- **Phase 3:** Directly take control of their behavior beyond the platform.

Players in the global netwar use this three-stage progression to take control of the behavior of individuals with memetic weapons. Memetic weapons utilize a number of cognitive vulnerabilities to facilitate behavior modification. These vulnerabilities include insights from the heuristics and biases approach, evolutionary psychology, neurolinguistic programming, and behavioral psychology. There are hundreds of distinct techniques which can be incorporated into memetic weapons. These include priming, the mapping of decision strategies, altering memories, and framing information based on evolutionary category systems. Effective memetic weapons will utilize a number of these vulnerabilities in parallel to achieve their desired results.

In the global netwar, individuals are pawns whose nervous systems are altered to co-opt their behavior. They are means to geopolitical ends. This view is not limited to Russia, as China's program of **Artificial Intelligence (AI) driven global sentiment management** demonstrates.

While most of the people who make up the networks on which this global war is fought are ignorant of its dynamics, they are not immune to its effects.

In addition to memetic weapons, the players in the global netwar use trolls and bots as front line troops in the social media battle space. Trolls play a support role to the memetic weapons—increasing their propagation, persistence, and impact. Trolls disrupt, amplify, and open people to the effects of memetic weapons. Bots accelerate the proliferation of memetic weapons, and act to affect the network dynamics which control their diffusion. The understanding of trolls and bots is the last piece needed to understand the dynamics of the global netwar in the social media battle space.

4.2 TROLLS

Within the social media battle space the trolls are the troops. Trolls are players who directly interact with individuals online, providing more nuance than a widely distributed memetic weapon.

NATO has stated that Russia has specific 'troll armies' which focus on different information battle fronts in the global netwar. Places like Ukraine, Latvia, Finland, and the United States each have an army of trolls in Russia specifically focused on their national information space. Venezuela, Iran, Syria, and China have also been accused of using troll armies. Sources state China's troll army consists of over 500,000 individuals.

NATO has identified five types of trolls frequently employed to influence memetic dynamics:

○ **The Aggressive Troll** posts aggressive messages and threatens individuals online. Aggressive trolls seek to disrupt information networks by eliciting emotional responses from individuals. This disrupts memetic exchange and creates structural holes in domestic networks which facilitate the isolation of individuals. Aggressive trolls disrupt specific narratives and specific memes while leaving others untouched. This allows them to control the narrative structure of a given information environment.

○ **The Bikini Troll** distributes e-memes which alter i-meme responses of individuals, and specifically targets men. Bikini trolls have attractive woman (frequently in a bikini) as their profile picture. They take advantage of the cognitive vulnerability men have to attractive women to distribute e-memes in comment sections which make targets more susceptible to memetic weapons. These are generally along the lines of "*Surely it is not only Russia that is bad?*" Focus groups have found these trolls are very effective at influencing males.

○ **The Wikipedia Troll** posts information from Wikipedia. Their comments lack any emotive valence and come across as flat and analytical. The information is always true, but used out of context to make the audience draw false conclusions. This helps populate information spaces with memes that add legitimacy to weaponized narratives, seeding e-memes which support the propagation of future memetic weapons.

○ **The Attachment Troll** posts very short messages whose goal is to get individuals to follow a link to another website. These sites are sophisticated weaponized information environments engineered to alter the target's belief system. The attachment troll seeds ties which connect benign information environments to the heart of the global netwar.

Their comments are framed as kindhearted attempts to 'educate' their audiences.

- **The Blame U.S. Troll** blames everything on the United States—specifically the CIA—from the Zika virus to the Indian Ocean tsunami. Claims are designed to be unfalsifiable, and consequently persist indefinitely. The Blame U.S. troll propagates e-memes which fragment western networks by sowing distrust in the United States, and Western narratives in general. They are the most effective trolls at influencing younger audiences.

NATO found that the people most susceptible to trolls are over 26 years old and settled into lifestyles with routines and responsibilities. Individuals over 50 years old were found to be especially susceptible to trolls. NATO found that younger users were generally more internet literate, and therefore less likely to get hooked by trolling attempts.

The only troll which has significant influence on younger users was the Blame U.S. troll—seeming to indicate younger audiences are most susceptible to conspiracy theories. These trolls play supporting roles to the memetic weapons which dominate the social media battle space. Trolls attempt to increase the susceptibility of individuals to these weapons and disrupt memes which could counteract the narratives these weapons are part of. They are frequently used in coordination with bots to amplify their effects.

4.3 BOTS

Bots are algorithmic entities which act in the social media battle space to amplify the propagation, persistence, and impact of memetic weapons. They are used in conjunction with trolls and memetic weapons in pursuit of geopolitical goals beyond the platforms on which they operate. David Beskow and Kathleen Carley at Carnegie Mellon have analyzed a number of bots online and identified several key types which act in the social media battle space:

- **Amplifier Bots** amplify the propagation of e-memes by pushing content. An amplifier bot retweets messages or specific hashtags to propagate e-memes throughout an information network. They can seed e-memes, support the persistence of narratives, and propagate memetic weapons through retweeting and liking specific posts or topics to distort the cyber mediated memetic environment.

- **Social Influence Bots** alter network topology by manipulating the algorithms social media companies use to regulate their platforms. They are able to accomplish this due to the low staff-to-content ratios which force platforms to rely on algorithms. These bots specifically target the algorithms which prioritize memes in the infinite scroll. They can be used to increase density, fragmentation, bridge structural holes, and prepare networks for memetic weapons by mentioning, following, commenting, and retweeting content. The difference between an Amplifier Bot and a Social Influence Bot is the goal of these behaviors. Amplifier Bots focus on memes, Social Influence Bots focus on network topology.

- **Intimidation Bots** target specific individuals to push them off of social media, eliminating their e-memes and narratives from the information network. This reduces competition for the behavior of individuals by eliminating competing memes from the information environment. Intimidation bots have bombarded reporters with lewd and disturbing images until they delete their social media accounts.

- **Coordinated Bots** are networks of bots which act in unison. These can be sets of any of the above bot types.

- **Cyborg Bots** are accounts which have both human and bot activity, and appear to represent individuals acting symbiotically with algorithms in pursuit of their goals.

These types of bots have been linked to Russian, Chinese, and Iranian information operations. Detecting and mitigating them is a large part of modern social cybersecurity. Bots help sculpt social media networks towards the ends of players in the global netwar. The primary goal of this sculpting is to create attack vectors for memetic weapons. Once an individual's behavior has been co-opted, they become a dupe.

4.4 DUPES

Most of the behavior which contributes to the goals of players in the global netwar is produced by individuals whose behavior has been modified by memetic weapons. These individuals have been transformed into dupes for foreign governments and unknowingly further the geopolitical goals of our enemies.Dupes are programmed to act algorithmically like bots,and frequently engage in behaviors which are not in their best interest or the best interest of their countries.

Russian intelligence has created a number of U.S. American dupes to support their netwar goals. These dupes have served as content creators for disinformation websites, photographers at Russian inspired protests, combat instructors for other dupes, and hosts for a regular Youtube show.Much of the global netwar is carried out in this way through proxies. These dupes lack the context to understand how their behavior fits into geopolitics and view their behavior as the result of their independent decision making processes.