MEMETIC WARFARE - PART II

Hacking Hearts and Minds

How Memetic Warfare is Transforming Cyberwar

OPEN Publications

Volume 1 I Number 6 I Spring 2017

OPEN PERSPECTIVES EXCHANGE NETWORK

This page is intentionally blank.

OPEN Publications (2017-06) Memetic Warfare – Part II

Hacking Hearts and Minds:
How Memetic Warfare is Transforming Cyberwar

OPEN Editorial Team

OPEN Contributing Author: Jeff Giesea[1]
OPEN Managing Editor: Robin Barnett
OPEN Editorial Review Board: David Beckwith and CAPT Mark Stoops

DISCLAIMER: OPEN publications are produced by Allied Command Transformation Operational Experimentation; however OPEN publications are not formal NATO documents and do not represent the official opinions or positions of NATO or individual nations. OPEN is an information and knowledge management network, focused on improving the understanding of complex issues, facilitating information sharing and enhancing situational awareness. OPEN products are based upon and link to open-source information from a wide variety of organisations, research centres and media sources. However, OPEN does not endorse and cannot guarantee the accuracy or objectivity of these sources. The intellectual property rights reside with NATO and absent specific permission OPEN publications cannot be sold or reproduced for commercial purposes. Neither NATO or any NATO command, organization, or agency, nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

Let us know your thoughts on Memetic Warfare – Part II by emailing us at natocde@act.nato.int or by posting your comments to www.openpublications.org

[1] Jeff Giesea is an entrepreneur based in Washington, DC. He published a related article, "It's Time to Embrace Memetic Warfare," in the first issue of NATO's *Defence Strategic Communications* journal and has consulted on numerous online PR and marketing campaigns. Giesea has BA and MA degrees from Stanford.

This page is intentionally blank

"One withstands the invasion of armies;
One does not withstand the invasion of ideas."
– Victor Hugo

This page is intentionally blank.

Contents

This page is intentionally blank.

Introduction

At a recent hearing about information warfare and possible Russian meddling in the U.S. election, the most revealing statement came from Michael Lumpkin, former head of the State Department's Global Engagement Center:

"To date, there is not a single individual in the U.S. government below the president of the United States who is responsible and capable of managing U.S. information dissemination and how we address our adversaries in the information environment."

To many observers, it has become obvious that Russia, China, and even the Islamic State are out-maneuvering the U.S. and allied governments in their use of information warfare and online propaganda, which I refer to as memetic warfare. What is notable, and damning, is how little we are doing about it.

Information warfare is "a conflict we have largely ignored," confessed Subcommittee Chairwoman Elise Stefanik at the same hearing. "What remains clear is that the cyber warfare and influence campaigns being waged against our country represent a national security challenge of generational proportions." She added that the hearing "brought to the fore the need to consider national-level strategies to counter state-sponsored propaganda efforts."

Some at the hearing supported the idea of recreating a United States Information Agency-type organization to help counter propaganda, an idea that former Director of National Intelligence James Clapper floated in January. Others suggested bringing back the Active Measures Working Group, a cross-government team the Reagan administration created to address Soviet propaganda at the end of the Cold War.

At a separate hearing days later, NATO's Supreme Allied Commander, Army General Curtis Scaparrotti, delivered a similar message to the Senate Armed Services Committee. The U.S. and NATO need to do more to counter Russia's propaganda and disinformation activities, he emphasized.

The political will to address cyber-enabled information warfare, it seems, is finally arriving. It is safe to assume we will see greater attention to these issues going forward, hopefully in a manner that rises above the bickering of domestic politics. But will it work? Can the U.S. and allied countries neutralize the threat of foreign online propaganda and gain the upper hand? Can we successfully work through all the legal, bureaucratic, and doctrinal issues involved? How should we even think about this?

In this paper, I'd like to offer memetic warfare as a much-needed paradigm shift to expand our way of thinking of cyberwar, and also as a tactical and operational tool for addressing these issues. To date, cyberwar has focused on hacking computers and networks, overlooking cyber-enabled efforts to influence hearts and minds. It is becoming painfully clear, however, that we cannot talk about cyberwar without including memetic warfare — defined here as information operations and psychological warfare conducted through the Internet and social media. In today's hyper-connected Information Age, the ultimate battle space is over our beliefs, narratives, and ways of viewing the world — in other words, our *memes*.

As lawmakers discuss strategies for countering foreign propaganda and building up memetic warfare capabilities, there is a lot to learn from the online trolling community. This paper offers some of these lessons. It concludes with several practical recommendations.

An Evolving Information Environment

Before going into these issues, it is important to appreciate how much the global information environment has changed and how rapidly it continues to evolve. This is all the more important before defaulting to Cold War-era solutions to today's challenges, or even those of the last decade.

Take a moment and think back to 2004 when, four days before the American election, Osama Bin Laden released a video taking responsibility for directing the nineteen hijackers responsible for 9/11. "People of America," Osama Bin Laden said, "this talk of mine is for you and concerns the ideal way to prevent another Manhattan…"

Even though the video had inferior production quality and less shock value than we are accustomed to today, and even though Bin Laden released it through Al Jazeera instead of Internet channels, there was something novel about a non-state insurgent leader communicating with the world in this way, in what felt like real-time. It was not quite a live Internet event as we experience them today, but one could sense a shift in paradigm in the manner of al-Qaeda's cross-continental propagandizing. From the confines of a cave in Afghanistan, he delivered a message received around the world. Anyone over age thirty can recall the image of him from that video, in his long beard and turban.

Fast forward to 2017, and we see conflict being fought through a globalized, rapidly evolving communications revolution. Anyone with a smart phone or computer has real-time access to global audiences with the swipe of finger or the typing of thumbs. This includes everyday citizens at home and college students in their dorms, as well as far-flung insurgencies, terror organizations, militaries, and non-state entities. The volume of images, symbols, and stories exchanged on social media is beyond comprehension.

When Bin Laden made his 2004 video, social media barely existed. Today it feels inescapable. Indeed, 20 percent of the global population has a Facebook account. The average adult spends 22 percent of all media time on social media, averaging over 5 hours per week. The number of global smartphone users grew from less than 50 million in 2005 to more than 2.5 billion today, while Internet users now top 3 billion. Add to this a growing presence of bots.[2]

Anyone wanting to broadcast globally, as Bin Laden did, can simply pick up their phone and live-stream through Periscope, Facebook Live, or YouTube Live. Likewise, anyone wanting to follow a political movement, or "shitpost"[3] on behalf of a candidate in another country, can easily do so.

The real-time, globalized, participatory nature of today's information environment is dizzying. It knows no borders and increasingly dominates how we make sense of the world. Disparate ideologies can rub shoulders and butt heads like never before, and anyone can participate. It is a propagandist's dream.

Russia and the Need to Expand our Paradigm of Cyberwar

In this context, cyberwar has taken on pressing importance for democratic nations. However, nearly all discussion of cyberwar in the West overlooks information and psychological warfare. These are secondary at best, and usually ignored altogether. Instead, cyberwar is defined in relation to hacking sensitive information, attacking critical infrastructure, or stealing intellectual property. In other words, the Western conception of cyberwar focuses on computers, networks, and infrastructure rather than ideas, culture, ideology, or public opinion.

Robert A. Clarke, in his seminal book *Cyber War*, exemplifies this narrow view. He defines cyberwar as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption." It seems obvious that nation-states are not the only ones engaging in cyber-attacks. Criminals, terrorists, journalists, leakers, and other non-state actors are some of the biggest perpetrators. Further, Clarke defines the object of attacks as computers or networks. He does not consider influence campaigns or efforts to shape public opinion as a component of cyberwar, either independent of cyber-attacks or in conjunction with them.

In the 2016 Worldwide Threat Assessment, former U.S. Director of National Intelligence (DNI) James Clapper points to cyber as the leading threat but makes the same oversight. Here is his summary of the cyber threat:

"The consequences of innovation and increased reliance on information technology in the next few years on both our society's way of life in general and how we in the Intelligence Community

[2] Bots are software programs that run automated tasks on the Internet. On social media, bots typically refer to fake users: they look like real, human users but perform automated tasks like spreading certain messages. Botnets refer to a network of connected and coordinated bots that work together. It has been alleged that Russia used Twitter bots and botnets to spread certain messages during the U.S. election. Independent U.S. citizens have done so as well.

[3] "Shitpost" is a slang word used among Internet trolls. It means to actively post and promote views on social media and in chat forums, often in an aggressive or trollish manner. I am using here to emphasize the reality that Internet trolls located anywhere can promote candidates in foreign elections through social media.

specifically perform our mission will probably be far greater in scope and impact than ever. Devices, designed and fielded with minimal security requirements and testing, and an ever-increasing complexity of networks could lead to widespread vulnerabilities in civilian infrastructures and US Government systems."

Note how the DNI focuses on infrastructures and systems. There is no mention of the threat of influence campaigns in the U.S. election or propaganda that weakens our trust in government itself. There is no mention of the threat of leaks. A year later these oversights feel tragic and almost laughable.

The level of resources allocated to information warfare and counter-propaganda reflects this mindset. Lumpkin pointed out that a single drone strike could cost up to $250 million, while total annual funding for the Global Engagement Center was below $40 million with less than $10 million spent on counter-terrorism messaging. In other words, annual counter-terrorism communications efforts are resourced at less than one-fifth of the cost of a single drone strike. Information operations are "mired in the bowels of the bureaucracy," Lumpkin explained.

By contrast, countries like China and Russia are actively investing more resources in information warfare and view it as an important tool in their spectrum of warfare. Matthew Armstrong, a strategic communications expert who was on the board of the Broadcasting Board of Governors, summarized the situation as follows:

"Today Russia, China, and the Islamic State lead prominent efforts to subvert, to confuse, and to divide their opposition while in the West, and the United States in particular, remains largely unarmed in this struggle for minds and wills."

Russia's aggressive approach, in particular, underscores the need to expand our paradigm of cyberwar and is worth a deeper look. Indeed, some say Moscow's use of propaganda is reaching levels of activity not seen since its Soviet days. There is significant documentation of Moscow's use of online propaganda to influence politics in the Baltic States, to assist the annexation of Crimea, and to facilitate its invasion of the Ukraine. Tactics have included using trolls and bots to spread disinformation, silencing and harassing dissenting journalists, and branding enemies as fascists and radicals. Additional tactics have included building up pro-Kremlin voices domestically and abroad, hiring pro-Russia trolls to spread messages and harass opponents, and using corporate troll farms like Internet Research Agency.

For example, a former employee of Internet Research Agency recalls being directed to write 135 comments about how then-President Obama chewed gum in India and spit it out. The idea was to denigrate him with a thousand paper cuts. And when Finnish television journalist Jessica Arko investigated Russia's troll armies, she herself became the target of attacks. In Crimea and the Ukraine, Russia coordinated social media propaganda as it deployed "little green men" in unmarked uniforms, displaying its skills in hybrid operations.

Some Russian communications have a sensibility that can only be described as trollish. Russia's former envoy to the NATO once tweeted an image contrasting a masculine Putin carrying a leopard with a weak Obama holding a small fluffy dog. The tweet said, "We have different values and allies." The Russian Embassy in London has sent similar tweets taunting British Prime Minister Theresa May with an image of Pepe the Frog, and then-President Obama with an image of a lame duck. On April Fools' day this year, the Russian Foreign Ministry posted an audio file on its Facebook page with a new switchboard message for Russian embassies: "To arrange a call from a Russian diplomat to your political opponent, press 1. Press 2 to use the services of a Russian hacker. Press 3 to request election interference."

In a paper called "Hacking into the West: Russia's Anti-Hegemonic Strategy and Strategic Narrative Offensive," authors James Rogers and Andriy Tyushka shed light on Russia's deeper strategy. They claim that Russia is engaged in a negative spoiler strategy that seeks to divide, distort, and desynchronize their western competitors, sowing chaos and confusion that leads them down paths they otherwise wouldn't follow. Russia cannot fight with the West through conventional warfare, the thinking goes, so why not use asymmetrical information warfare and wreak havoc without ever firing a shot. Rogers and Tyushka describe this as an "anti-hegemonic strategy" of chaos and disruption designed to diminish self-confidence and create disorder. One element of this is to saturate the West's narrative space with false and fictitious stories. A related paper in the same journal goes into the conceptual roots of Russia's approach. Evgeny Messner's concept of "subversion-war" and Aleksandr Dugin's concept of "net-centric war," for example, elevate the informational and psychological dimensions of warfare and marry it with ideological and meta-political vision.[4]

In a recent RAND report called "The Firehose of Falsehood," authors Christopher Paul and Miriam Matthews summarize Russia's propaganda model as follows:

> *"In some ways, the current Russian approach to propaganda builds on Soviet Cold War-era techniques, with an emphasis on obfuscation and on getting targets to act in the interests of the propagandist without realizing that they have done so. In other ways, it is completely new and driven by the characteristics of the contemporary information environment. Russia has taken advantage of technology and available media in ways that would have been inconceivable during the Cold War. Its tools and channels now include the Internet, social media, and the evolving landscape of professional and amateur journalism and media outlets. We characterize the contemporary Russian model for propaganda as 'the firehose of falsehood' because of two of its distinctive features: high numbers of channels and messages and a shameless willingness to disseminate partial truths or outright fictions."*

Russia, it could be said, is at the leading edge of state-sponsored memetic warfare, and China seems to be following a similar playbook. This does not mean the U.S. and allies should mirror their approach, but it does call for a rethinking in order to contend with it. Other actors are watching. We cannot afford to turn away our eyes.

[4] Dugin is particularly worth studying given his influence with Putin. His 1997 book, *Foundations of Geopolitics*, has become a sort of geopolitical textbook for modern Russia. His 2009 book, *The Fourth Political Theory*, lays out his vision for a new, post-liberalism political theory.

Memetic Warfare as a Strategic Reframe

The most powerful re-conception we can undertake to address this is to expand our view of cyberwar to include memetic warfare, the informational and psychological battles waged online. It is critical that we think of cyberwar as a fight over our hearts, minds, and narratives — our *memes* — as well as our computers, network, and infrastructure. Some background on memetic warfare and meme theory may help elucidate.

In 2015, I wrote a paper for the NATO StratCom Centre of Excellence (CoE) entitled "It's Time to Embrace Memetic Warfare." The paper defined memetic warfare as "competition over narrative, ideas, and social control in a social-media battlefield." It made the case for memetic warfare as a guerilla subset of information operations tailored to social media. The paper discussed some of the legal, bureaucratic, doctrinal, and ethical issues associated with making memetic warfare a reality. It also pushed for more aggressive education and experimentation:

"For many of us in the social media world, it seems obvious that more aggressive communication tactics and broader warfare through trolling and memes is a necessary, inexpensive, and easy way to help destroy the appeal and morale of our common enemies."

I was not the first to develop the concept of memetic warfare. Michael B. Prosser, a Marine Corps officer, mentioned it a decade earlier in his 2006 paper, "Memetics: A Growth Area Industry In US Military Operations."

The concept of memetic warfare has roots in meme theory. In the context of social media, many people think of memes as funny images with text across them. However, the term meme is a much broader and deeper concept coined by Richard Dawkins in his 1976 bestseller *The Selfish Gene*. In simplest terms, memes are units of cultural transmission — behaviors, ideas, styles — that spread from person to person. Dawkins attributes cultural evolution to the most successful memes, stating: "Memes are to culture what genes are to life. Just as biological evolution is driven by the survival of the fittest genes in the gene pool, cultural evolution may be driven by the most successful memes."

Memetics is the study of memes and information transfer. It draws from a variety of fields such as evolutionary psychology, neuroscience, marketing, and biology. Memetics is less interested in the truth of a meme than its ability to spread and influence. The trends, expressions, and ideas we share are all forms of memetics.

The ability to spread or replicate is essential to the concept of a meme. Dawkins often refers to memes as replicators. Building on Dawkins' work, Francis Heylighen, describes meme-replication as a four-step process. First there's assimilation, when a meme "infects" a new host. The second stage is retention, when a meme sticks and is retained in memory. The third stage, expression, is the communication of a meme in a unit of information that others can understand.

Finally there's transmission, when a meme spreads from one person to another through a conduit like a book, TV, or the Internet.

Heylighen, with Klaus Chielens, defines meme fitness as the overall success rate of a meme as a replicator. In mathematical terms, meme fitness is a function of the success of a meme at each of the four lifecycles. Thus, when designing shareable units like talking points or advertisements, one can use memetic fitness as a framework to help gauge potential success. "Fake news," for example, is an example of a recent meme. It stuck, it spread, and it shaped the dialogue. Its biggest failure has been its ability to hold its form. In typical memetic warfare maneuvering, the term has been coopted and weaponized against the very media entities that coined it.

A related field worth mentioning is social physics. Social physics uses big data to study social learning and idea flow, and how they impact beliefs, behaviors, and productivity. In his book *Social Physics*, MIT professor Alex Pentland writes: "We must stop thinking of people as independent decision-makers, and realize that dynamic social effects are equally important at shaping our ideas and are the driving force behind economic bubbles, political revolutions, and the Internet economy." Social physics, in sum, quantifiably demonstrates how social networks impact the spread of memes.

With this theoretical background, one might think of memetic warfare is as cyber PSYOP. Cyber PSYOP is about influencing the attitudes and actions of others by dominating narratives through channels of cyberspace. The most effective narratives are spread by memes. When we weaponize memes, we get memetic warfare.

One can consider memetic warfare as a component of cyber PSYOP, to illustrate what it does and how it is waged. Yet even the cyber PSYOP label can be misleading. The cyber part of memetic warfare is different from cyber warfare, because the target of the attack is the minds of the target audience. Cyber is just the delivery system into those minds. Therefore, memetic warfare is a form of psychological combat waged mainly through online information. But unlike PSYOP, memetic warfare is not simply a tactical-operational tool but a form of strategic information warfare.

As mentioned previously, memetic warfare does not yet fit Western military thinking, but it should. To offset aggression in today's information environment, we must recognize that hacking hearts, minds, and culture is just as important a form of warfare as the ability to hack computers. We must align our defense capabilities accordingly.

Memetic Warfare Campaign – A Hypothetical Example

Memetic warfare is about advancing specific objectives to specific audiences through specific tactics in online communication. In this sense, a memetic warfare campaign is not unlike an advertising or PR campaign, though the mindset and tactics are quite different.

As a thought experiment, let’s pretend a foreign government wanted to weaken American public support for NATO. The target audience is the American public, though one might segment efforts around specific demographics such as “America First” Trump supporters or leftwing anti-globalists. The desired effect is to weaken U.S. support for NATO, with a specific objective around reducing favorability opinions. A secondary objective could be for the messages to spread to Europe, where they instill fear and uncertainty in the Alliance and stoke division between member states.

Memetic warfare tactics in this scenario could include everything from a #PullOut hashtag campaign advocating pulling out of NATO (imagine a sub-set of these including vile and pornographic images with #NATOhasAIDS messages); funny images denigrating NATO troops, soldiers, and leadership; news analysis of American citizens’ per-dollar spending on NATO relative to other countries, with shareable charts; targeted anti-NATO talking points in key gathering places for this audience (comment sections, chat boards, etc.); an influencer network of NATO skeptics who help spread key talking points; an army of bots to signal boost these messages; and carefully placed fake news stories about NATO being a sign of the anti-Christ and the New World Order targeting, say, religious older women.

Other tactics might include trolling influential pro-NATO voices; commenting on articles with anti-NATO messages; organizing and Periscoping (live-streaming) rallies in front NATO buildings; publicly releasing leaked information from NATO employees; and conducting research and investigative reporting to develop stories that make NATO look bad. The list goes on.

This brainstorm isn’t intended to be particularly good or advanced, just illustrative. Many of these tactics are not considered ethical or respectable within our societies, and that is partly the point of this exercise: Memetic warfare is warfare. We have to prepare for the worst. Our adversaries will not always play by the same rules we do, so at the very least we need to stretch our imaginations and ask: How do we defend against this?

It is critical to note that very few of these tactics involve breaking any laws, and none of them involves violence or kinetic combat. Moreover, the entire campaign could be passed off as a PR campaign, or conducted from abroad, or financed by the billionaire friend of a prime minister rather than being funded directly by a government. Much of it could be done anonymously or through surrogates. Plus, various citizen groups would likely latch on to the campaign and contribute to it in their own ways. Pinpointing acts of war in this context is complicated. The lines blur.

Memetic warfare, one might say, is the Wild West of asymmetric conflict. It is dirty. Attribution is complex. As with any type of warfare, there are important moral, legal, and doctrinal dimensions to consider that go beyond the scope of this paper.

Lessons from Internet Trolls

There is one community at the leading edge of memetic warfare in today's information environment: Internet trolls. By trolls, I mean the denizens of chat boards and social media who operate as sort of guerilla warriors of Internet trends and memes.[5] Governments seeking to defend against foreign online propaganda and develop memetic warfare capabilities may want to look to this community for guidance on strategies, tactics, and organizational methods.

At first blush, it may seem that wedding the impulses of aggressive keyboard warriors with the discipline and centralized nature of standard military practice is like encouraging a union of fire and ice. But if one includes trolling and memetics in the spectrum of warfare, then this fusion becomes both plausible and necessary. Learning from the Internet hiveminds of 4chan, Reddit, 8chan, Twitter, or any other distributed network of trolls is, in essence, no different than learning the ways of any other set of guerilla soldiers. For that matter, it is not very different from engaging with hackers.

Thus, the intention here is not to glorify nefarious forms of trolling behavior. It is simply to share a few lessons from this community that could help allied governments put memetic warfare into practice. The lessons that follow tend to be organizational in nature, not tactical. They are intended to start a dialogue, not to be definitive or all encompassing.[6]

Perhaps the most important lesson from the troll community is that excessive hierarchy does not work. Effective memetic warfare requires speed, adaptability, and a high degree of creative independence. Because of the velocity of information on the Internet — i.e. what is trending, what people are talking about, what is in the news cycle — the capacity to run decisions up a chain of command is nonexistent. Rather, a fire-at-will culture prevails among trolls, who instantly overwhelm slower, more deliberate adversaries with different vectors of attack and faster information loops. Thus, attempting to bureaucratize memetic warfare in a typical command-and-control structure will not work. Distributed models of warfare, like Fourth Generation Warfare and open-source warfare, are likely to be more effective. Think networks, not organizations.

Furthermore, many trolls place a high value on independence and autonomy. In fact, the less formal leadership there is, the better. This is not merely because of the anti-authoritarian mindset of trolling communities, but also for a simpler tactical reason — because memetic warfare often relies on intensely personal attacks. The 12th rule in Saul Alinsky's famous political organizing handbook *Rules for Radicals* is to "pick the target, freeze it, personalize it, and polarize it." Trolls achieve this *par excellence* against their targets. Retaliation is often

[5] Although trolls are often regarded as annoying and toxic, this paper views them more broadly as guerilla warriors of information. As with any guerilla, some trolls operate with noble objectives, others for entertainment, and others for nefarious reasons.

[6] These lessons are intended as observations rather than conclusive facts. I welcome feedback.

impossible, since troll campaigns are often carried out by faceless mobs of anonymous Internet users. Elevating a visible, formal leader can make the entire operation vulnerable.

Leadership in the trolling world, to the extent it is recognized, is informal and understated. Formally appointed, hierarchical leaders are generally non-existent. During the Gamergate controversy, for instance, one fact that infuriated journalists and activists was that the movement had no leader. The movement actively mocked the concept by jokingly anointing irrelevant figures "the leader of Gamergate." Such tactics increase the fog of war and enable memetic warfare operations to remain constantly on the offensive, with no obvious vulnerable spots for counterattack.

The take-away for governments is that memetic warfare works best when conducted through flat, fluid, headless collaboration structures, rather than rigid, hierarchical organizational structures. Harvard Business School Professor Amy Edmonson's concept of "teaming" comes to mind as a way of thinking about this. Software development practices like Agile and new Blockchain-based methods of collaborating, such as Backfeed, are other places to look.

A second lesson from trolls is the importance of experimentation and creativity. As mentioned previously, the term meme originates from evolutionary biology. Like organisms seeking survival, memes must come optimized to stick and spread, lest they end up relegated to such digital obscurity.

To give an idea of how difficult survival in these environs is, consider the case of 4chan, arguably the *fons et origo* of modern trolling culture. On 4chan's most popular board, the Random or /b/ board, only 15 (originally 10) pages of latest posts are ever visible. According to some estimates, 4chan receives 18 million unique visitors a month, the majority of whom likely spend at least some time on /b/. As such, that number of people trying to post in such a limited amount of space produces a stream of content too fast for normal users to maintain. Therefore, if a user wants their work to remain visible on 4chan for longer than a very short space of time, the user must constantly try to send different iterations of their content through the site, hoping that enough users will react to at least one version that it might remain up for longer than a few solitary minutes.

This is an extreme example, but the point stands: For memetic warfare to be successful at a strategic level, it often has to go through multiple iterations of failure at the tactical level. Therefore, room must be made for experimentation and creative freedom. The freer the hand of the operator at a tactical level, the more likely it is that that person will find a way to achieve the objectives. Elite trolling, some might say, is a form of art. And memetics is a form of culture creation. Thus, governments interested in these crafts would be wise to look at studios, agencies, and other models of cultural influence for inspiration.

This brings up a third lesson — that memetic warfare is as much an ethos as a craft. The ability to "speak Internet," in addition to understanding the nuances of the target audience, is important to anyone wanting to engage in memetic warfare.

The Internet is a subculture unto itself, or rather collections of subcultures. These sub-cultures have their own norms of behavior, language, and sensibilities. Within certain sectors of the troll community, phrases like "lulz," images of Ron Paul waving his hands saying "it's happening," and quotes from the fictional super-villain Bane are all part of an ever-evolving cultural short-hand. Among the center-right trolls who supported Trump and Brexit, phrases like "praise Kek" and images of Pepe the Frog are ways of signaling membership and of speaking a common language.

An old catchphrase among trolls is "the internet is serious business." Despite its obvious truth in many circles, the phrase is intended with dripping irony. One conceit of the communities most skilled in trolling is that things said or done on the Internet are inherently unworthy of concern in real life, rather like a game with no rules other than getting a laugh. In other words, in the world of trolling, the rules of engagement and social norms of "normies" (normal people) are more often objects of ridicule than reverence. Trolling comes with its own set of norms, but it is by its very nature unregulated and is often successful to the extent that it is willing to break rules. Thus, broadly speaking, it is best to assume that a particular societal norm is inoperable until proven otherwise. Many trolls refer to their craft as "weaponized autism," and this is not necessarily meant as an insult. Never underestimate the power of weaponized autism, the thinking goes.

This gets to an equally important point about ethos: trolls view the Internet as a fundamentally low-trust environment, perhaps as we all should. Newcomers to existing communities are generally regarded with suspicion at best, and outright hostility at worst. It is telling that the 4chan-generated insult "newfag" is meant to be insulting because of the "new" part, rather than the slur at the end. Gaining trust within such communities is a process, and one that is spoiled by violating community norms. Even beloved "leaders" who arise organically from within the community can sometimes end up despised if they act with too much self-arrogated authority or are perceived as taking more credit than deserved. Thus, when engaging in these circles, it is important to cultivate trusted relationships, to rely on persuasion rather than coercion, and to error on the side of humility. Trust, influence, and reputation are currency.

A fourth lesson in memetic warfare from trolls is to rely on organic rather than paid distribution of memes and ideas. When trolls speak of "meme magic," the reference to magic is not incidental. Like the best magic, successful memetic warfare hangs on belief in the ability to manifest reality — a faith in memes, if you will, combined with the legwork and creativity to unleash them and a network of influencers to share them. If a meme cannot stick and spread on its own, the thinking goes, it is probably not a worthy one. Kek did not will it. Indeed, nothing will more easily ensure a meme's being held up as an object of ridicule than the perception that it is "forced." Likewise, attempts to command other trolls to spread one's content, no matter its quality, risks being met with the timeless rebuke that they are "not your personal army."

Because of the reliance on organic distribution, many trolls operate with the mindset that attention equals influence, no matter whether it is good or bad attention. It is quite telling, for instance, that the act of trolling almost always refers to attempts to engender negative reactions, rather than positive ones: trolls understand instinctively that strong negative reactions are just as likely to polarize people over content as the content itself. In other words, memetic warfare sometimes takes the phrase "there's no such thing as bad publicity" to its most extreme conclusion; better to have bad publicity that forces people to pay attention than lukewarm good publicity that they ignore.

Elements of the media have validated this strategy. The phenomena of hate-reading and hate-sharing have both received mainstream press attention, and both can be very good for the bottom line of publications that benefit from them. In the realm of politics, President Trump's tweets achieve success in pushing his message in part by virtue of his ability to provoke furious reactions among traditional media gatekeepers, who inadvertently keep his messages in the public eye as they denounce them.

Further, because angry reactions to provocative content are likely to be provocative themselves, a strategy of seeking attention regardless of its positive or negative quality can be highly effective in producing unrest within enemy communities. Witness the phenomenon of "concern trolling," wherein a user attempts to infiltrate a community whose values they disagree with, only to then raise "concerns" about the community that provoke internal dissension among its members. Violating a community's norms, meanwhile, often draws the most visibly offended members, whose excesses in responding may in turn disenchant more moderate peers more than the original violation. In short, for trolls, it often pays more to be the bad guy than the good guy.

The take-away for governments is that memetic warfare tends to favor insurgent forces over established ones. Disrupting is easier than promoting. Resources do not give as great as an advantage as in conventional combat, and adversaries are not likely to be bound by the same rules that you are.[7]

A fifth and final lesson from the troll community, at least in this brief section, is to rely on open-source approaches to action, decision-making, and intelligence gathering. A recent example of these skills in action concern Hollywood actor Shia LaBeouf's "He Will Not Divide Us" campaign. LaBeouf, in response to persistent 4chan-sponsored attacks on his "He Will Not Divide Us" art exhibit, which was intended to exist in opposition to President Donald Trump for the duration of the latter's term in office, decided to move a flag bearing his slogan to an "undisclosed location," with only the sky and the flagpole visible.

4chan's /pol/ board took this as a challenge and leaped into action to find the flag and take it down. Eventually, through a combination of checking flight patterns, employing astronomical measuring devices, and on-the-ground surveillance, all coordinated spontaneously through 4chan itself, anonymous trolls were able to track down the location of the flag in Tennessee and replace it with a "Make America Great Again" hat and a Pepe the Frog t-shirt. This process took them only a few days. As one person tweeted: "The US government couldn't find Osama bin

[7] The flip side of this is that "digital counterinsurgency" may be a useful way to think about defensive memetic warfare.

Laden for 6 years, but 4chan found the #HWNDU flag in a field in the middle of nowhere in 37 hours."

After that loss, LaBeouf moved his exhibit to Liverpool, England, where he hoisted a flag and live-streamed a protest, only to be foiled once again by trolls, who scaled rooftops to capture it. Now people are guessing that LaBeouf and his cohorts will move their project to Helsinki, where once again the global presence and collective intelligence of trolls will take aim. What began as a prank has effectively turned into a war-gaming exercise for collaborative trolling, pitting 4chan trolls against LaBeof's quest to keep his campaign alive.

The open-source model of allowing the maximum number of users to not only have access to information, but to mine it for discoveries, flies in the face of traditional intelligence gathering. Yet it shows the power of crowdsourcing, possibly even masking actual intelligence gathering with the appearance of spontaneous civilian grassroots activity. Certainly, this was achieved when massive troves of Wikileaks data were linked directly to Reddit's The Donald board during the 2016 election cycle, at which point users motivated solely by their self-proclaimed "weaponized autism" combed through all the data and discovered relevant, actionable pieces of information with incredible consistency and speed.

The lesson for governments is to approach memetic warfare with an open-source mindset. Explore innovative approaches to using the Internet and social networks to solve problems. Consider platforms for viral collaboration. Sometimes it is better to let an army of non-professionals do the work rather than a few experts.

While the trolling community speaks to us from a culture whose prickly anti-authoritarianism seems at odds with military practice, their approach also offers distinct advantages that are integral to successful memetic warfare: speed, adaptability, creativity, psychological insight, spontaneity, collective intelligence, anonymity, and more. This is not to say that Internet trolls are superior in all aspects of memetic warfare. Their use of behavioral data and analytics tools, for example, is non-existent relative to the digital advertising world. But that being said, U.S. and allied governments would be wise to look to Internet trolls as capability experts. There is much to learn from them.

Conclusion and Recommendations

In November 2014, then-Secretary of Defense Chuck Hagel announced a once-in-a-generation Defense Innovation Initiative called the Third Offset Strategy. The plan aimed to develop new strategic capabilities that give the U.S. continued asymmetrical advantages in conflict.

In a paper entitled "Twenty-First Century Information Warfare and the Third Offset Strategy," James R. McGrath argues that the Third Offset Strategy does not adequately address the need for advanced information operations. He writes:

"For U.S. forces to achieve the Third Offset Strategy, the joint force must be able to achieve information superiority at the time and place of its choosing. To do that, the joint force must develop innovative operating concepts for IO [information operations], war-game them using a variety of computer-based methods, and then train to the newly discovered tactics, techniques, and procedures that are absolutely essential for 21st-century warfare—a type of warfare aimed at breaking the will of the adversary through control of the IE [information environment]."

McGrath is spot on. In the current environment, we are playing catch up to adversaries that are out-maneuvering us in information warfare, which we only dubiously recognize as warfare and for which we have no effective answer. But is achieving McGrath's wish for sustained superiority in the realm of memetic warfare a realistic objective, particularly as we uphold ethical ideals against adversaries who take a no-holds-barred approach? Is the ability to "break the will" the correct objective? How do we defend against influence campaigns without trading one type of propaganda for another, or without diminishing the health and freedoms of our civil societies? What does this look like in a scenario of non-linear memetic warfare, where allegiances and attributions are fluid and murky, where domestic actors mix with foreign state and non-state actors, and where anonymity makes it hard to it is hard to tell who is who?

This paper offers memetic warfare as a paradigm shift in the way we think about of cyberwar, and as a strategic and tactical tool for helping address foreign online propaganda. It also builds a bridge to different sources of operational knowledge like the trolling community. It has become increasingly obvious that existing approaches to countering foreign propaganda are dated, under-resourced, and ineffective in today's complex, hyper-connected, and ever-swirling information environment. We need fresh thinking. We need to approach memetic warfare with the same level of commitment as other forms of combat, particularly in a defensive capacity. No single magic bullet, like recreating the U.S. Information Agency (USIA) "on steroids" is going to solve this.[8] Likewise, simply mirroring the tactics of less encumbered adversaries is not likely to be effective.

Making meaningful progress will take a combination of efforts. Here are four recommendations for where we might look next.

First, NATO and member governments should create task forces directly responsible for addressing the issue of foreign online propaganda with specific recommendations for dealing with it. These task forces should include public and private voices, be free of domestic politics, and have clear mandates. For example, the U.S. task force could be charged, among other things, with delivering recommendations that specifically address each of the hurdles to effective counter-measures that Michael Lumpkin mentioned in his testimony: "lack of accountability and oversight, bureaucracy resulting in insufficient levels of resourcing and inability to absorb cutting-edge information and analytic tools, and access to highly skilled personnel." Existing cyber and information operations capabilities may be advanced and highly effective, but how can we better utilize them?

[8] In fact, the State Department, where the USIA was previously housed, may be among the least optimal places to house memetic warfare capabilities.

Second, more investment needs to be made in identifying the tactics of foreign governments and non-state entities, understanding their impact, and proving that they were utilized and attributable. What if the impact of foreign active measures is less than we think? Or more? What if we can definitely prove guilt or not prove guilt? What if the hysteria over Russian propaganda is just that? Finding answers makes a big difference in how we can respond, and right now we do not seem to have the definitive intelligence needed for a more fact-based discussion. Thus, we must attempt to close this knowledge gap. This effort should be conducted in coordination with social media platforms and independent, non-partisan research teams. New technical solutions may be needed to solve attribution challenges. We may find that "sunlight is the best disinfectant" when it comes to memetic warfare activities, that exposure is the best deterrent. After all, exposing and verifiably attributing acts of memetic warfare gives governments grounds to respond in any number of ways, including bombing the propagandists or imposing international sanctions on the state.

Third, NATO and member governments should invest in more doctrinal work and experimentation through newer, more agile vehicles already immersed in the *lingua franca* of memetics. One way to do this would be by sponsoring an independent innovation lab and research institute that brings forth knowledge from a cross-section of private citizens, a sort of real-life Bureau of Memetic Warfare.[9] This new institute could provide more rapid guidance on questions like: how can citizens help diminish the propaganda value of terrorism? It could further develop intellectual concepts like "digital counterinsurgency," which may be a useful framework for neutralizing memetic warfare from ISIS and others. It could also sponsor prize contests similar to the DARPA Red Balloon Challenge[10], host conferences that bring together people from different fields, and oversee innovative experiments and "skunk works" projects free of government command and control. Providing resources to accelerate these types of endeavors is likely to pay off handsomely.

Fourth, and finally, NATO and member governments should enhance internal training on memetic warfare. Basic education and awareness-building about memetic warfare — what it is, why it matters, how to identify it — would help give people a common language, bridge generational divides, create a foundation for policy doctrine, and bring to surface new sources of expertise and innovation. For more advanced training, memetic war-gaming may be valuable: pit a team of Internet trolls against a government team and see what happens. This sort of tactical memetic warfare training may be a valuable addition to existing cyber and information operations training programs, as well as those involving military intelligence, counter-terrorism, and public diplomacy.

Memetic warfare awareness shows that this type of combat is everywhere, and growing. The U.S. and other NATO members would be wise to smarten up quickly. In the trolling world, there is a saying that if you control the memes, you control the world. It is time for our national security apparatus to let that sink in.

[9] This is the name of a discussion board on 8chan.

[10] The winning team from MIT made use of viral collaboration similar to the way Internet trolls do.