IT'S TIME TO EMBRACE MEMETIC WARFARE

Jeff Giesea

'The best way to counter ISIS is to unleash an army of trolls on them', Charles C. Johnson joked over beers last spring. 'I could totally mess with their recruiting and propaganda.'

Johnson is known as one of the Internet's biggest trolls, the social media equivalent of an annoying gadfly or guerrilla warrior, depending on one's perspective.[1] He's been banned from Twitter and is alleged to have spearheaded the rumors that triggered the downfall of the all-but-certain Speaker of the House of Representatives, third in line for the American presidency.[2]

During our carousing, Johnson and I joked about different ways to troll ISIS or Daesh. One could systematically lure and entrap (i.e. 'catfish') Daesh recruiters, as three Russian girls did in early 2015.[3] One could water down its recruiting propaganda using fake 'sockpuppet' Daesh accounts, creating hall-of-mirrors confusion for sympathizers and recruits.[4] One could expose and harass people in Daesh's funding network, including their family members.[5] One could even play on Daesh's prejudices, fears, and hypocrisies, enlisting gay activists worldwide to start and spread an #ISISisgay hashtag, the idea being to denigrate and ridicule Daesh in a way that weakens its appeal to recruits.[6] The list went on. 'These types of tactics are no-brainers,' we concluded half-jokingly. 'So why aren't they being done?'

1 Articles on Johnson: Mother Jones, 16 Dec. 2014, 'The Rise & Fall of Twitters Most Infamous Right-Wing Troll' (http://www.motherjones.com/politics/2014/12/charles-chuck-johnson-gotnews-rolling-stone); Gawker, 9 Dec. 2014, 'What Is Chuck Johnson, and Why? The Web's Worst Journalist, Explained' (http://gawker.com/what-is-chuck-johnson-and-why-the-web-s-worst-journal-1666834902); Slate, 28 May 2015, 'Why Did Twitter Ban Charles C. Johnson?' (http://www.slate.com/articles/technology/users/2015/05/chuck_c_johnson_suspended_from_twitter_why.html)

2 Gawker, 8 Oct. 2015, 'Source: Kevin McCarthy Affair Rumors Have Been Circulating for Months'.

3 Yahoo, 29 July 2015, 'Catfished! Girls Scam ISIS on Social Media for Travel Money' (https://www.yahoo.com/travel/catfished-girls-scam-isis-on-social-media-for-125374397897.html).

4 Some refer to this as a 'hall of mirrors' strategy.

5 Brookings, 24 Oct. 2014, for insight on ISIS funding, 'Cutting Off ISIS Cashflow' (http://www.brookings.edu/blogs/markaz/posts/2014/10/24-lister-cutting-off-isis-jabhat-al-nusra-cash).

6 One could get the public and gay groups involved in a denigration campaign, sharing memes like these (https://imgflip.com/login?redirect=/creations) and captioned videos like this one (http://www.liveleak.com/view?i=f08_1424123423) (nsfw).

Obviously, this was lighthearted banter with no strategic frame or focus. But 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.

The term 'memetic warfare' has come into use on the fringes of foreign policy thinkers in the last five years to describe these types of efforts.[7] I believe memetic warfare could be effective in countering Daesh's recruiting and propaganda efforts and in modern conflict in general, including operations other than war. Trolling, it might be said, is the social media equivalent of guerrilla warfare, and memes are its currency of propaganda. Daesh is conducting memetic warfare. The Kremlin is doing it. It's inexpensive. The capabilities exist. Why aren't we trying it?

It's no secret that the U.S. and NATO allies have done a poor job combating Daesh on social media thus far. In June 2015, the U.S. State Department conducted an internal assessment of its communications efforts that admitted that the NATO-led coalition is losing the social media war with Daesh.[8] Existing efforts like the 'Think Again, Turn Away' campaign have proven ineffective against the tide of outreach coming the other way. By mid-2015 there were an estimated 30,000 foreign Daesh combatants,[9] with the majority coming from NATO countries. Experts say Daesh's recruiting is reaching 'network effect' velocity, and much of it is conducted through Twitter, YouTube, and other social media. The need to counter Daesh's communications onslaught is urgent.

Kalev Leetaru makes a compelling case for a more muscular communication approach in a July article in *Foreign Policy*.[10] The article, 'A Few Good Internet Trolls', argues that more aggressive and comprehensive cyber communication efforts are needed as battlefields shifts online.

What Leetaru and others seem to overlook, however, is that selling the high-level concept is not the hard part. Political leaders already understand the need for a more

7 The first use I found was by Brian J. Hancock, 'Memetic Warfare: The Future of War' (https://fas.org/irp/agency/army/mipb/2010_02.pdf), Military Intelligence Professional Bulletin May-June 2010; also see Max Macrides, 'Freeing the Empire of the Mind: Memetic Warfare and International Strategy', unpublished paper, 2015.

8 NY Times, 12 Jun. 2015, 'ISIS is Winning The Social Media War, U.S. Concludes' (http://www.nytimes.com/2015/06/13/world/middleeast/isis-is-winning-message-war-us-concludes.html?_r=1).

9 NY Times, 26 Sep. 2015, 'Thousands Enter Syria to Join ISIS Despite Global Efforts' (http://www.nytimes.com/2015/09/27/world/middleeast/thousands-enter-syria-to-join-isis-despite-global-efforts.html?smid=nytnow-share&smprod=nytnow&_r=1&mtrref=undefined&assetType=nyt_now).

10 Foreign Policy, 14 Jul. 2015, 'A Few Good Internet Trolls' (http://foreignpolicy.com/2015/07/14/islamic-state-twitter-recruiting/).

aggressive approach, at least at an abstract level. The hard part is actually making it happen, of transitioning the abstract concept into reality and, in turn, victory. There are numerous obstacles standing in the way: conceptual ones, financial ones, cultural ones, legal and bureaucratic ones, and strategic ones.

Here are several things we need to do to overcome these obstacles. By pursuing these, we can bring to life smarter online strategic communication practices and adapt civilian practices that can help us defeat present and potential enemies like Daesh.

Develop Memetic Warfare Conceptually

The first challenge is conceptual. Neither NATO nor its individual members have fully developed a language or conceptual grounding for social media-focused Strategic Communications. Memetic warfare today is a fringe concept, but it shouldn't be. It needs to be developed and brought into mainstream military thinking.

In doing so, it should be thought of as broader and more strategic than 'weaponized trolling'. Memetic warfare, as I define it, is competition over narrative, ideas, and social control in a social-media battlefield. One might think of it as a subset of 'information operations' tailored to social media. Information operations involve the collection and dissemination of information to establish a competitive advantage over an opponent. Memetic warfare could also be viewed as a 'digital native' version of psychological warfare, more commonly known as propaganda. If propaganda and public diplomacy are conventional forms of memetic warfare, then trolling and PSYOPs are guerrilla versions.

Memetic warfare can be useful at the grand narrative level, at the battle level, or in a special circumstance. It can be offensive, defensive, or predictive. It can be deployed independently or in conjunction with cyber, hybrid, or conventional efforts.

The online battlefield of perception will only grow in importance in both warfare and diplomacy. Regardless of what we call it, NATO countries must continue to develop a body of knowledge around social-media Strategic Communications.

Allocate Better Resources to It

Greater investment – and better investment – is required, too. As NATO members continue to aggressively invest in cyber warfare and cyber security, they should also invest in memetic warfare.

Let's clarify how these areas relate. Cyber warfare involves attacking a nation's computers and networks to cause disruption or gather intelligence, or defending against such attacks. Examples include the Stuxnet virus that sabotaged Iran's nuclear program in 2010, or China's breach of the U.S. Office of Personnel Management files in early 2015 (and the U.S.'s response).[11] They involved no physical combat in the traditional military sense.

Cyber warfare is about taking control of data. Memetic warfare is about taking control of the dialogue, narrative, and psychological space. It's about denigrating, disrupting, and subverting the enemy's effort to do the same. Like cyber warfare, memetic warfare is asymmetrical in impact. It can be highly effective relative to cost. The attack surface can be large or small. Memetic warfare can be used in conjunction with troops, ships, aircraft, and missiles, or it can be employed without any kinetic military force at all. It operates in the communications battlespace.

The communications battlespace, of course, is where we are losing to Daesh. Ambassador Alberto Fernandez, former head of the U.S. State Department's Center for Strategic Counterterrorism Communications (CSCC), gave a frank assessment of communication efforts in an outgoing interview last year. 'It's not that ISIS is so great', he said. 'It is that the response to ISIS is both limited and weak.'[12]

If the communications battlespace is where we're losing, why aren't we investing more in it? Why has NATO placed itself in the position of responding to Daesh rather than having prevented Daesh and similar forces from existing in the first place? Why hasn't NATO gone on the offensive to wipe out Daesh and other jihadists as credible psycho-political movements? (The discussion of waiting until extremists become violent before they are countered — the essence of Countering Violent Extremism (CVE) initiatives — rather than forestalling their rise in the first place is another issue entirely, but it is one that can also be addressed through memetic warfare.) NATO and many of its members individually are investing some funds in strategic communications, with the U.S. State Department alone spending $118 million in 2015.[13] Yet the amounts, while impressive, are miniscule in proportion to what we're spending overall.[14]

11 BBC, 15 Feb. 2011, 'Stuxnet Virus Targets And Spread Revealed'; NY Times, 31 Jul. 2015, 'U.S. Decides to Retaliate Against Chinese Hacking' (http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html).

12 CBS News, 10 Jun. 2015, 'Flaws Seen In U.S. Approach to ISIS Propaganda' (http://www.cbsnews.com/news/flaws-seen-in-u-s-approach-to-isis-propaganda/).

13 Last February, the U.S. State Department funded a $188 million CVE initiative. See fact sheet 19 Feb. 2015 (http://www.state.gov/r/pa/prs/ps/2015/02/237647.htm).

14 Mother Jones, 14 Jun. 2015, 'Charts: How Much We're Spending On The War Against ISIS' (http://www.motherjones.com/mojo/2015/06/us-defense-spending-war-isis).

Even at current spending levels, one must question how effectively these resources are being allocated. The civilian funds directed toward CVE and communications are relying on public diplomacy and top-down 'conventional' Strategic Communications, with military information operations and PSYOP showing themselves to be tepid, timid, and stale. Where is there experimentation? Where are the guerrilla efforts? Where is the innovation? Where is the war-gaming of tactical successes at the Strategic Communications level?

NATO's communications efforts to date are like Version 1.0 of a software program. Releasing the first version is incredibly difficult and an accomplishment in its own right, but now it is time for version 2.0 and a more serious commitment to rapid learning and improvement. To get there, NATO and individual member countries must commit more physical resources and command authority to Strategic Communications, allocate existing spending more intelligently, and provide intellectual and operational space for learning and innovation.

Embrace the Memetic Mindset

Perhaps the greatest obstacle to memetic warfare is a lack of appreciation for social media as a battle space and the extent to which memetic warfare is already taking place. Perhaps this is generational: from the outside looking in, it doesn't appear that the alliance's military and foreign policy decision-makers truly understand social media at all, much less as a tool and weapon for the common defense. How many generals are active on Twitter and truly understand it beyond the explanations of their kids or younger colleagues?

Even for those of us who live on social media, it is sometimes difficult to appreciate how quickly information can spread, the profundity of its global scope, and the significance of its impact on perceptions, narratives, and social movements. Once one starts viewing the Internet through meme-colored glasses, you see memetic warfare everywhere — in political campaigns, in contested narratives about news events, in the thoughtless memes shared by Facebook friends, and in videos on YouTube. It shows up in movements like #BlackLivesMatter, where there's an attempt to shape perceptions and galvanize public support. In the U.S. Republican Primary race, Jeb Bush recently attempted to paint Donald Trump as the 'chaos candidate'. But when his campaign tried spreading a #ChaosCandidate hashtag, trolls supporting Trump took it over and used it to denigrate Jeb Bush.[15] Hashtags, one might say, are operational coordinates of memetic warfare.

15 See https://twitter.com/hashtag/chaoscandidate

On the geopolitical stage, memetic warfare is being used in a military capacity by centralized governments like China and Russia, in addition to non-state actors like Daesh. Anyone who has read the comments on news articles related to foreign policy has probably noticed some suspiciously inauthentic, biased comments. China employs 20,000-50,000 Internet police and an additional quarter-million 'trolls' who spread pro-Beijing material domestically and abroad, and who help monitor citizens.[16]

Similarly, Russia has 'troll farms' where Internet commentators spread pro-Moscow messages and disinformation. It tends to use memetic warfare offensively. It has been notorious in its disinformation related to Ukraine, from the 'green men' who were 'not' Russian troops, to the shoot-down of the Malaysian airliner, to the nature of the Ukrainian government itself. Moscow has also targeted domestic affairs in the U.S. In 2014, Russian trolls spread disinformation about a chemical plant explosion in Louisiana under the #ColumbianChemicals hashtag. They spread similar disinformation about an Ebola outbreak in Atlanta, under #EbolaInAtlanta. In each case, there were fake videos, photos, and Wikipedia pages, combined with outreach to journalists and buzz centered on a hashtag.[17] As the United States has downsized its information operations and PSYOP capabilities, the Kremlin's RT propaganda house has begun to recruit former professionals.[18]

A 'memetic skirmish' involving the U.S. Embassy in Moscow demonstrates that talented and creative State Department communicators are poised to act when allowed. In August 2015, the local news in Moscow released a photo showing U.S. Ambassador to Russia John Tefft conducting a press conference at an opposition rally. The photo, according to the U.S. Embassy, was a fake. It seemed to be deliberate disinformation. The Embassy had a brilliant response. 'Ambassador Tefft spent his day off yesterday at home', the embassy tweeted. 'But thanks to Photoshop, he could be anywhere.' Shortly thereafter, various Russian twitter accounts released the same press conference photo of Ambassador Tefft against a variety of backgrounds - landing on the moon, surrounded by cats, at various weddings, at a hockey game, landing in the Philippines with General MacArthur during World War II, and elsewhere. It became a meme, and Russia's disinformation effort backfired.[19]

16 American Political Science Review 5/13 'How Censorship in China Allows Government Criticism but Silences Collective Expression' (http://gking.harvard.edu/files/gking/files/censored.pdf)

17 NY Times 6/2/15 'The Agency' (http://www.nytimes.com/2015/06/07/magazine/the-agency.html); also Reuters 3/11/15 'EU leaders want to tackle Russian "disinformation" on Ukraine war' (http://www.reuters.com/article/ukraine-crisis-eu-idUSL5N0WD4JL20150311).

18 I will provide this source material soon.

19 For more info and examples of the memes, see BuzzFeed, 21 Sep. 2015, 'This Is The Best Photoshop The US Government Has Ever Produced' (http://www.buzzfeed.com/maxseddon/the-state-department-has-finally-learned-how-to-use-twitter?utm#.ssV4eV2Ln)

The Ambassador's Photoshop imbroglio recalls a meme from early in 2015, when Daesh was demanding $200 million in ransom to release two Japanese journalists. The terrorists released a photo of Jihadi John wielding a sharp knife above the heads of the two Japanese men, kneeling in orange jumpsuits. As the 72-hour deadline to pay the ransom passed, Japanese Twitter accounts began sharing doctored images of the threatening photo set against darkly comic backgrounds — one with Jihadi John holding a banana instead of a knife, another of him wearing Mickey Mouse ears and the Disney Magic Kingdom in the background, and another with him wearing pink lingerie in a field of flowers. The 'meme-ing' of the image was viewed as a symbol of defiance among the Japanese, a classic denigration. It did not save the life of journalist Kenji Goto, but it may have helped lessen the psychological impact of Daesh's propaganda.[20]

For memetic warfare to succeed, decision-makers need to get into the right mindset and empower those who have it. Study what's worked and what hasn't. Network across civilian disciplines, particularly with Internet trolls, hackers, marketers, and PR pros. To the extent possible, experiment on social media yourself or through those close to you. Try following and influencing an issue. Embrace memetic warfare as an essential capability in modern warfare.

No one is better to support this than the NATO Strategic Communications Centre of Excellence. I recommend organizing a cross-disciplinary global summit on memetic warfare. Consider focusing it specifically on countering Daesh and giving it the feel of a TED conference (perhaps partner with them), drawing fresh ideas, perspectives, and connections from multiple disciplines and countries.

Make Space for It Legally, Bureaucratically, & Ethically

As a thought experiment, let's pretend that a NATO member nation decides to experiment with counter-narrative strategies to blunt the appeal of Daesh ideology among Muslim males aged 15-35 in the Western world. Let's assume further that creating a viral #ISISisgay denigration campaign is deemed a tactic worth testing as part of a broader memetic war effort. How could this tactical effort be executed from a legal and bureaucratic standpoint in their political and cultural context? Let's look at some potential obstacles using the U.S. as an example.

20 For more info and examples of the memes, see DailyMail, 24 Jan. 2015, 'How Japan Is Fighting Back At Jihadi John With Memes' (http://www.dailymail.co.uk/news/article-2924504/How-Japan-fighting-Jihadi-John-MEMES-Images-ISIS-executioner-cutting-kebab-meat-posing-selfie-stick-viral-nation-shows-won-t-silenced-new-hostage-threat.html)

In the U.S., there are laws from the State Department and Broadcasting Board of Governors that expressly prohibit domestic propaganda. The trouble is, social media doesn't recognize borders. Would an #ISISisgay denigration effort be considered domestic propaganda as conducted on worldwide platforms like Twitter? Today it likely would. These laws, designed for a 20th century media environment, pose a significant structural challenge for memetic warfare, not to mention a convenient rationale for officials who do not want to get involved.

Even if legal hurdles were cleared, it's not clear which government agency would be in a position to conduct such a campaign. Would it come out of the State Department's Center for Strategic Counterterrorism Communication? The military? The CIA? Would it be done from within the government or through contracts with private companies? In the current environment, the only way this could occur from the U.S. is through a Title 50 contract as a covert intelligence operation, which would require a presidential finding. Even without these top-level barriers, how could the campaign be executed free from multiple layers of stifling bureaucracy? This is perhaps the more significant question.

Politically, #ISISisgay would be a sensitive campaign to execute. Even with thoughtful coordination with gay groups and other domestic interests, there would still be a risk of media and political criticism. Recall what happened in 2005 after the Pentagon awarded contracts worth $300 million for psychological operations to improve foreign public opinion about the U.S. abroad. The media discovered that the contractor, Lincoln Group, was planting stories in the Iraqi press. The perceived meddling became a political lightning rod.[21] For campaign like #ISISisgay, decision-makers are likely to be exceedingly gun-shy.

Ethically, it's not clear where to draw boundaries for this type of campaign. Is it ethically justifiable to spread homophobic and juvenile memes if it helps undermine and ridicule Daesh and its followers? Would the answer be different if the memes come from the gay community and 'Gays Against ISIS'-type groups? How does the possibility of unintended consequences factor into this, including the possibility that such a campaign inadvertently helps Daesh? Are NATO member nations too politically correct to use offensive themes to undermine mortal enemies?

Here is what seems odd about the current context: Today NATO members have the legal, moral, and bureaucratic setup to tear apart human beings with bombs, but not to fight them with social-media-focused Strategic Communication. Does this make

21 LA Times, 30 Nov. 2005, 'U.S. Military Covertly Pays to Run Stories in Iraqi Press' (http://articles.latimes.com/2005/nov/30/world/fg-infowar30)

sense? If we want to counter Daesh's digital outreach, NATO countries must make space for memetic warfare in their respective legal, bureaucratic, and ethical contexts. NATO's Strategic Communications Centre of Excellence can do two things two help. First, it can help initiate conversations about creating legal, bureaucratic, and ethical space for memetic warfare among member nations. Second, it can help member nations understand each other's operating environment in order to facilitate the sharing of best practices and the coordination of memetic war efforts. Indeed, one advantage of NATO is that member nations each have their own unique legal, bureaucratic, and ethical environments. If a certain type of campaign isn't feasible in one country, perhaps there's another country where it would be.

Keep Learning & Experimenting

Even with all of these unresolved issues, NATO member nations must continue experimenting with social-media-focused Strategic Communications in their respective operating environments.

The technology industry is known for mantras like 'test and measure', 'iterate rapidly', and 'move fast and break things'. The same mindset applies here. Yes, there are known and unintended risks to consider, particularly in a type of activity that flourishes with greater autonomy and less oversight. But as with a company facing a disruptive technology (think of Kodak with the rise of digital photography), member nations must adapt and innovate or get left behind. Except in this case, the consequences of inaction are much greater than bankruptcy, layoffs, and a loss of market share.

Indeed, the riskiest thing NATO members could do is to allow risk-aversion to hamstring the development of memetic warfare. To say a lot is at stake is an understatement, not just with Daesh but with Russia, China, Iran, and all the non-state actors watching Daesh's success from the sidelines. If a small non-state terror organization can outfox the wealthiest nations on social media, what does this signal to others? How many more lives will be lost and what will the world look like if Daesh's online recruiting continues unabated? The threat is civilizational or at least geopolitical. NATO member nations cannot afford to sit on the sidelines.

It's time to drive towards a more expansive view of Strategic Communications on the social media battlefield. It's time to adopt a more aggressive, proactive, and agile mindset and approach. It's time to embrace memetic warfare.