NS NARRATIVE STRATEGIES
CHANGING THE WAY POWER WORKS

A Five-Point Strategy to Oppose Russian ***Narrative Warfare***

(with the limited tools we currently have available)

Paul Cobaugh

April 2018

Image from the ***Beyond propaganda series****: Information at War: From China's Three Warfares to NATO's Narratives, September 2015*

Legatum Institute

Introduction

Before retiring from the US Army in late 2015, I spent most of my career in a community which had as one of their mantras, albeit an unwritten one; **that when presented with a problem, "don't just complain, present solutions".** This paper is just that, a discussion of pragmatic and recommended solutions for protecting ourselves from Russian narrative/ information warfare.

This paper is intentionally written in narrative form rather than the usual linear strategy format. We are after all, talking about narrative warfare. It is also written as plain-spoken as possible so that everyone from policy-makers and national security strategy professionals through well-informed citizens can follow the discussion.

Abstract

Influence, done well is a complex and intricate choreography of sustained actions, words and related activities wrapped around a ***core narrative****. Russia, in our current global security arena is aggressive by way of campaigns with just such choreography. National, regional and individual security dictates that we develop and execute a strategy to effectively deal with such aggression… and do it promptly. While there has been a great deal of talk and hand-wringing within the USG (US Government) on this topic, to date, no comprehensive and executable strategy exists.*

Given that influence has become Russia's weapon of choice, influence operations by default must become the primary strategy of resistance and containment. The USG and most of our Allies have largely ceded the influence battlefield to Russia, offering only token resistance. Of note, many other nations and non-state actors such as DAESH are also executing similar strategies against the US and our Allies with varying degrees of intensity and success. Developing an effective strategy for Russia by default would go a long way towards addressing these other threats as well. Implementing a complete strategy and the massive reworking of USG security architecture as required would be time prohibitive considering the current level of threat and even worse, risky. Pragmatic solutions focused on more effective and aggressive use of the tools we do have now would dramatically improve our defenses.

The following strategy recommendation is not revolutionary; it is sheer, common-sense pragmatism. It also is not entirely unfamiliar to long-time US influence professionals, since as a nation, the US was once quite proficient at managing influence warfare. Sadly, post-Cold War, we have allowed our prior prowess to become a rusting relic of our past. Of additional importance in reclaiming our prowess is the default requirement for training a new generation of influence practitioners adept at the art and tradecraft of influence.

Please remember, this paper only addresses the bare-boned minimum strategy, its five must-do lines of effort and based on the tools we have at hand. Along the way, some of the glaring inadequacies in US information warfare trade-craft, doctrine and architecture will be highlighted as well. If we are to cage the aggressive Russian bear, this discussion is merely step one. Evolving US influence capabilities, architecture and training with vision and expedience is step two. Both steps will be painful but necessary if we are to remain safe and competitive on the world stage.

Contents

Framing the problem

Let’s begin by framing the problem. There is a significant, ongoing and unconstrained threat emanating from Russia which I and my colleagues at Narrative Strategies characterize as “Narrative Warfare” or as most people from influence/strategy professionals down through informed citizens call it, ”information warfare”. Regardless of the name attached to this type of conflict, the threat is most simply defined as a war, yes, a war of *influence* with narrative at its core. Despite the current consternation over what to call this type of warfare, what is missing is not the name but the strategy to effectively engage in and protect ourselves.

So-called “fake news”, propaganda, mis/disinformation, conspiracy theories and so on are not plunked down into the US cognitive environment randomly. Each tweet, online post, RT (Russia Today) news story etc. is carefully designed to support a specialized and highly influential type of story called a narrative. These narratives and their sub-components are designed to exploit vulnerabilities and trigger predictable behavior in US and Western audiences in order to diminish our collective ability to resist Russian aggression. This narrative warfare is an integral and central part of Russia’s overall campaign of malign influence against us. To date, Russia operates with near impunity as the US and our Allies have yet to formulate and execute a comprehensive strategy with which to defend ourselves. This failure is partially due to the fact that Western nations don’t clearly understand narrative warfare and have allowed our former Cold War prowess in information warfare to fall by the wayside. Failure to understand influence warfare also means by default that until we do, strategy development cannot be effectively accomplished.

Why “narrative warfare”?

Narrative warfare is, in its simplest explanation and by default, influence. In a war of influence, the object is to use all available means to **trigger predictable behavior** favorable for your side. The question then becomes “what” is the object of triggering behavior? States, non-state actors and individuals are perpetually attempting to influence audiences to align with their perspective when they employ influential tactics. At a minimum, the audiences they cannot align are influenced to at least offer no opposition. The intent of this alignment is predictable influence and hence dominance over adversaries and competitors.

As an example, during the Cold War, two opposing belief systems were competing to align audiences with socialism/communism or democracy. Both sides employed a narrative extolling the virtues of their “side” punctuated by events which were then “spun” to support the narrative. The “war” itself was over which belief system was to dominantly endure. This included shaping the identities of those targeted to align with the intended belief system and to erode confidence in the adversarial system. The battles of influence within the war and selected influence weapons used were over individual portions of the overall narrative. Make no mistake, it was never about the battles, it was about the war itself and by default, which narrative would win.

Narrative is a specialized story that gives meaning to a set of facts, events or associated information expressed as truth. The single most effective reason narrative is so powerful as a tool of influence is because narrative is all about identity and meaning, rather than truth. When narrative is employed based on the art and science of narrative, it triggers predictable behavior based on the identity of the targeted audience.

“Life stories do not simply reflect personality. They are personality, or more accurately, they are important parts of personality, along with other parts, like dispositional traits, goals, and values,” writes Dan McAdams, a professor of psychology at Northwestern University, along with Erika Manczak, in a chapter for the APA Handbook of Personality and Social Psychology.

So, if narrative is the intent, the vehicles for delivering narrative based content are social and traditional media. It's not just the media employed but the media in conjunction with delivery methods in support of the narrative that must be impacted or displaced in order to defend against a virtual, media-based narrative assault.

At a minimum, there are multiple measures which can and should be taken by DoD and the USG as a whole in order to displace adversarial dominant narratives, disrupt adversarial content and delivery of narrative-centric content. These basic measures must also be integrated into a strategy as unilateral measures will not accomplish the mission of mitigating the threat. To date, there is no such comprehensive effort. So, as with the earlier quote regarding complaining and solutions**, I submit that at a minimum, the five following efforts need to be at the core of our strategy.**

1. **Build resilience in US audiences that aids in recognizing and resisting influence.**
2. **Apply CYBER tools proportionately, both offensively and defensively.**
3. **Regularly disseminate effective alternate and counter-narratives.**
4. **Message by all available and appropriate means, messaging in support of our narrative strategy.**
5. **Deterrence or rather: Demonstrate by action that aggression will be firmly resisted.**

I. Resilience

"Resilience is the process of adapting well in the face of adversity, trauma, tragedy, threats or significant sources of stress — such as family and relationship problems, serious health problems or workplace and financial stressors. It means "bouncing back" from difficult experiences."

"Resilience is not a trait that people either have or do not have. It involves behaviors, thoughts and actions that can be learned and developed in anyone."

As characterized by The American Psychological Association

The reason that resilience is first on the list is simply because "hardening" our personal defenses against influence is the core of the issue. In military parlance, a "hardened target" is difficult to penetrate. If mis/disinformation don't penetrate, their effects are by default mitigated. A cornerstone of Russian influence operations is false and misleading information disseminated through various channels. Its intent is to deceive, divide and erode adversarial resistance to their aggression. As their targets are primarily civilian audiences, it becomes essential to "harden civilian targets" to the effects of such activity.

Resiliency is in fact the process of hardening these targets. First and foremost, this requires educating audiences and divorcing them from "identity politics" or adversarial narratives which are so influential in exploiting such politics.

Tactics, either defensive or offensive, are either protecting your side or attacking the will of an adversary. As an analogy it's helpful to look at resilience much the same as taking protective measures against infection by a communicable disease. Washing hands, avoiding infected people and places or employing all manner of protective measures contribute to resilience and cumulatively mitigate and manage the risk of infection and exposure. Malign influence, such as currently and aggressively employed by Russia has no absolute cure, hence minimizing the risk is a critical, pragmatic and partially achievable option.

Building resilience in a political landscape as divisive as we currently have in the US is difficult but not unobtainable. As an indicator of just how important this is, we can only look at how many resources Russia applies to promoting and exploiting divisive topics. If it were not important, they would spend their time and resources elsewhere.

"Since everything is up for interpretation, in information warfare the worst position to be in is defensive..."

Alicia Wanless and Michael Berk

The question regarding resiliency is mostly centered on "how to mentor citizens to resist emotional and divisive content that is inaccurate and harmful". A recent article in the Washington Post discusses the approach that Sweden is employing to "inoculate" voters against Russian narrative warfare. In the article, the focus is on how opposing political parties are both committed to educating and mentoring all voters, not just those politically aligned, to recognize, report and expose media focused on malign influence by Russia. Resiliency is everyone's responsibility.

Resiliency recommendations against Russian malign influence:

- Such an approach requires more than lip service by leadership from both sides of the political divide. It also requires resources. Faith in national institutions such as law enforcement, the intelligence community and the military are non-negotiables as well. Voters go where leaders follow and thus it becomes a requirement for leadership to drive these requirements and like the old adage; "lead by example".

- "Hardening" a unified national identity by solidifying our core values, by default reduces the threat of divisive narrative warfare. "Who we are as a nation" is based on our historical narrative. This identity, once hardened, reduces the threat from weaponized and divisive narratives from Russia and other aggressors. Again, identity as a critical component of narrative, is key. Like the old adage regarding feuding siblings who will fight each other but band together to resist outside threats, the US populace must do the same. Our internal issues are for us to sort out without allowing outside threats to exploit our divisions. Like the siblings, we can disagree fervently with each other but must not allow foreign malign actors to “have a say” in our domestic problems.

- US political parties would have us believe that there are two primary identities and that they do not share common values. Though this is a common perception, it is far from the truth. Both Political “sides” have a responsibility to establish this unified, though often at odds identity. Though there are differing opinions, sometimes dramatically, both sides still adhere to the common core values which revolve around our Constitutional principles. Leaders that constantly pit one side against the other as “un-American” dangerously provide Russia with the opportunity to further exploit our differences for their own purposes. Intentionally pitting one side vs. the other is not only dangerous, it is un-American. Remember, “divide and conquer” is one of the oldest and most effective of military strategies. Why should we make Russia’s job easier by allowing them to do so?

- Education, regarding digital literacy, though a much longer approach is a critical element of resiliency. Students and all adults have the responsibility of citizenship to be accurately informed. One of our most trying problems with mis/disinformation is that it is easier to accept content that bolsters our identity regardless if it is true, accurate and in context. A large number of Americans now habitually believe that “winning for their political side” is more important than solving a problem. This must stop! Learning to fact-check, do credible research and apply critical analysis are all hallmarks of a resilient populace. Education and mentoring regarding these three elements are the responsibility of schools, parents, community leaders etc. Curriculum and teaching techniques must be instituted in our schools and public institutions beginning at a very early grade level and be supported by parents and other respected community leaders. Facts, in context matter.

- Public and credible renunciation of false and miss-leading content by trusted leaders and institutions is a “must-do”. Challenging all “fake news” or otherwise is required consistently, not only when it “helps” your political/ social beliefs. I cannot emphasize this point enough. Leaders from the local level through the highest office have a citizen’s responsibility regarding accurate, in context information. Those who fail in this aspect of resiliency have no business in a leadership role.

- Finally, while there currently is a great deal of focus regarding social media, it is only one aspect of resiliency. Speed and global reach though have given social media an outsized role in modern influence operations. Another aspect which the CA (Cambridge Analytica)/ FB (Facebook) debacle has brought to light is of critical importance in narrative-centric information warfare, data. Enough data analyzed provides a deep look at “who we are” individually and in tribalized groups of voters. Going back to the critical role of “identity” in narrative influence, data in the hands of experienced analysts provides the primary way to unlock the identity of those being influenced. This simply means that protecting our data also has a key role in building resiliency to influential SM.

II. CYBER, both offensive and defensive

Like it or not, the majority of the globe is now connected digitally and this is in regards to our personal lives every bit as much as national, regional or international infrastructure. Defeating digitally-based infrastructure once required massive kinetic campaigns but now can be impacted with literally the touch of a button or key on a keyboard. Furthermore, systems can now be impacted temporarily or without lasting harm, therefore limiting the impact to affected populaces. Such disturbances are a potent message to those impacted much like sending an extortion message by a mafia enforcer when they want to enforce compliance with the wishes of the “Don”. We must both protect ourselves from the “message” and the intrusion in order to provide the deterrence which protects us from such extortion.

Russia has and continues to target digital infrastructure both public and private. For sensitive reasons, I will not delve deeply into portions of this topic but denying access to bad actors is a critical aspect of any future strategy to mitigate Russian aggression. This is true regarding access to sensitive information as well as into social media platforms, etc. The tools exist. They must become employed more effectively and **fully integrated** with all other aspects of cognitive security. (Lydia Kostopoulos P. , 2018) Also, most critical is the issue of emerging technology on the digital battlefield. We must be first, be ethical and ultimately, most effective if and when we defend or deter by way of CYBER.

Offensive CYBER, has a wide-spectrum of opportunity. One of the most significant is the application of “deterrence” attacks. This is much like walking up to the biggest bully on the playground and punching them in the nose. Without that action, there is no reason for the bully to alter their behavior. Yes, actions are messages, too and in Russia’s case, these are messages they will well understand. This is more than simple deterrence. Offensive CYBER must deliver a message that demonstrates consequences. As is often quoted in defense legal realms, CYBER is often construed legally as act of war. The subtle distinctions of such though are very much in play and taking the risk adverse position presents no opportunity to “punch the bully in the nose”. There is a very wide gray area between massive CYBER attacks against national resources and infrastructure and proportionate “messages” of deterrence along with proportionate consequences.

“You cannot only defend in cyberspace,” said Erki Kodar, Estonia’s undersecretary for legal and administrative affairs who oversees cyber policy at the defense ministry.

Offensive and Defensive CYBER recommendations to mitigate Russian aggression

- **Defensive**
    - Deny access to US and Allied institutions and individuals by Russian state and non-state actors by technical means.
    - Identify, expose and neutralize malign digital actors and their resources.
    - Protect sensitive information both personal and institutional.
    - Deploy measures that identify bad actors and their “tools” of intrusion/attack.
    - Automate defensive technical measures to respond to threats.
    - Expand Intelligence oversight authorities to allow for protective measures in regard to US citizens and residents.
    - Support global authorities to identify and prosecute bad actors, state or non-state.

    - Institute strict and enforceable regulations with commercial institutions with access to data and its use.
    - Dedicate a perpetually evolving entity to analyze emerging threats and implement counter-measures along with the requisite legal authorities to do so.

- **Offensive**
    - Strategize and proportionately employ offensive deterrence measures that make CYBER attacks/ intrusions cost prohibitive for adversaries.
    - "Giving an adversary a taste of their own medicine" proportionately is most certainly a deterrent with the emphasis on "proportionate".
    - Selective targeting of infrastructure, military, commercial and individual that demonstrates consequences is a very clear signal that adversaries are vulnerable as well should they be determined to be unrelenting in their use of CYBER.
    - Penetration into adversarial dissemination outlets even though they have been blocked, limited and/ or deemed illegal provides deterrence as well. As an example, Russia restricts access to internal media by Western media to a large extent in order to protect themselves from precisely the same tactics they employ against the West.

III. Regularly disseminate our own compelling narrative as well as counter-narratives to adversarial narratives

As noted at the outset, large-scale influence campaigns are by default, **Narrative Warfare**. These weaponized narratives along with all supporting efforts in such a campaign are oriented towards the meaning set out in an adversary's narrative. Such meaning loosely or sometimes specifically identifies an adversary's intended objectives of their campaign. While in military planning parlance, objectives, courses of action, restraints/constraints etc. have specific meaning, it is unhelpful to adhere to the very narrow definitions of military planning. Most military planning is linear in nature. Influence is dimensional in nature. Using one to achieve results in the other is the planning equivalent of attempting to "put a square peg in a round hole". The bottom line to this is that planning matters. The right type of planning matters more… and executing the right plan with the required resources matters the most.

Remember, narrative is about identity and meaning. Narratives, well-constructed deliver meaning to a series of issues and events so that audiences don't sort the meaning out on their own. Merely disseminating sterile press releases (PRs) will not accomplish furthering our agenda since they typically only provide facts. PRs. though are excellent supporting messages to an over-arching narrative if well-constructed to deliver meaning, rather than sterile facts. Meaning is critical in that both Allies and adversaries are often confused by our disparate actions and words simply because we have not bothered to explain the meaning of our words and actions. Both Allies and adversaries need to clearly understand what we're doing and why.

The inherent risk of only messaging isolated and unrelated facts without attaching meaning is that the adversary has the opportunity to attach “their meaning” to the same facts. This means you’ve allowed the adversary, in this case Russia, to control the meaning of events, factual or otherwise.

In terms of the role of narrative, offensive and defensive, it is important to understand some basic differences in narrative terminology. The following three explanations matter the most in a strategy:

“Weaponized Narrative”

The term “**Weaponized Narrative**” **(WN)** has come into relative prominence in the wake of Russian efforts against the West. WN is a piece of an overarching narrative strategy. WN, a specialized type of narrative is designed to fill the cognitive space that specifically targets the vulnerabilities of an adversary by establishing “meaning, not facts” which triggers behavior, sustains the initiative, and crowds out competing narratives. Once established, simply countering such a narrative is very difficult without a compelling narrative of your own.

In the case of Russian meddling in the US and other Western nations, the Russian narrative or as discussed later, “family of narratives” were designed to trigger predictable behavior in the identity of separate and opposing elements of Western society as well as “sell” Russian legitimacy for their acts of aggression in places like Ukraine and Syria.

Weaponized narrative is powerful because it targets predictable behavior by way of emotional responses, most often fear. This subset of WN can often be described as “conflict narrative”.

Operational Or Comprehensive Narrative Strategy

Operational Narrative or a comprehensive narrative strategy is a complete package of both offensive and defensive narratives coordinated to both degrade adversarial audiences and to build resilience within friendly audiences. When thinking about a complete narrative strategy, a good analogy is a sport such as football that includes both offensive and defensive strategy and more importantly, a game plan which encompasses both.

As with any sporting event, the team must play both offensive and defense, execute a game plan and play at a superior level if your team is to win. Not employing any of these elements most often results in a loss for your team. In the case of Russia vs. many Western nations, this has been and still is to some extent the case. Simply put, Russia is deploying a powerful offensive or weaponized narrative strategy with impunity and largely unopposed. Their vulnerability though is that they are not playing much defense except by insulating their populace from a Western narrative by restrictive measures such as isolating friendly audiences and by technical methods such as CYBER.

“Family of Narratives”

FoN (family of narratives) is a far more complex but requisite construct. I will try and simplify as much as possible and again use Russian information warfare as the example.

Russia does not only deploy a WN that says they are good, honest and strong while contrasting the West as weak, divided and a threat to themselves and others. In order to "sell" this idea they use a great many sub-narratives such as designed to:

- Highlight divisive issues in Western society such as:
    - Migration
    - Nationalism
    - Racial issues
    - Economic disparity
    - Hypocrisy
    - Etc.…

- Russian strength and legitimate rights such as:
    - Russian involvement in Ukraine is based on a distorted right to assert protection of Russians at risk from a corrupt Ukrainian government.
    - Russia is the good and loyal friend of Syria wishing only to destroy terrorists and support the rightful government,
    - NATO is encroaching on Russia's western border and is a threat.
    - Etc.

These sub-narratives are what are best described as a family of narratives. All speak to different identities of different audiences, all portray meaning, not truth and all are delivered in a form most suited to triggering predictable behavior in each audience. All support their overarching narrative and attendant themes and most importantly, each "family member" supports the family narrative as a whole.

With the above understanding, US/Allied influence strategy must employ a comprehensive narrative strategy as described in the portions; "**Operational Narrative and FoN (Family of Narratives)".**

How we accomplish this then becomes the question. This question also identifies one of our US most critical vulnerabilities. The US, since the demise of the USIA (US Information Agency) in the mid-1990s and the side-lining of Strategic Communications in 2012 at the Pentagon, has lost critical players responsible for strategic narrative. The Pentagon and Office of the Secretary of Defense have largely tried to make up for these losses by shifting to a Public Affairs (PA) approach and dependence on the US Department of State (DoS). Neither is currently capable of handling the delicacy nor volume of the task.

Asking PA and DoS alone to manage the strategic narrative task is the military equivalent of telling a political candidate to manage dissemination of their platform and communications by a couple of PAOs and a handful of highly placed friends and without the benefit of media, messaging and related actions under the control of a campaign manager. To make matters worse within the US, most IO related entities self-victimize by way of sibling rivalry over budgets, roles and tasking authority.

Narrative dissemination must be controlled by a central USG coordinating authority that has much the same command and control (C2) as a media service managing a significant political campaign or a marketing firm with global customers. The current architecture of the USG is deficient in nearly every possible way to achieve operational narrative dominance. As that a full-scale narrative strategy must be integrated across strategic, operational and tactical levels simultaneously and responsively, the FoN (family of narratives) concept is nearly impossible without a centralized C2 mechanism.

An aspect of narrative warfare frequently forgotten is that it requires its own unique type of intelligence collection and analysis. Narrative identity analysis (NIA) is not synonymous with target audience analysis (TAA). Typical TAA is centered essentially on demographics/ preferences. Narrative identity analysis is centered on literally, the identity of the audience. Sentiment analysis employed by some marketers, is closer but still not focused on “who the audience” truly is and identifies as. Understanding how to trigger specific identity is precisely the point of influence.

Recommendations:

- Create, staff, and authorize tasking authority to a single USG entity charged with developing, disseminating and assessing strategic communications to include narratives and supporting messaging:
    - This single entity would be civilian lead with a board comprised of senior leaders from DoD, DoS and all other relevant entities including the IC (Intelligence Community)
- **Create a comprehensive narrative strategy that includes a FoNs (family of narratives) that speak to multiple and disparate audiences, friendly and adversarial. Base all narratives on the core principles/ science of narrative: 1. Narrative identity 2. Meaning, not fact 3. Structure/form.**
- Designate a core analysis community of IC professionals that can:
    - track, analyze and assess dissemination of narratives.
    - Identify unique audiences and based on narrative principles undertake NIA (narrative identity analysis).
- Create a digital TF (task force) with innovative and current technology that collects, analyzes and assesses dissemination of narratives friendly and adversarial.
- Create a sub-component that synchronizes a US narrative strategy with friendly nations and non-state entities.
- Ensure that a comprehensive approach to messaging can be achieved to accommodate long and short term (responsive) messaging requirements.

VI. Message by all available and appropriate means and message in support of our narrative strategy

Routine and regular messaging in support of the meaning contained in the narrative strategy means that you are managing and controlling the conversation. This is dominance in military-speak. Much like an awkward and disjointed conversation in a social setting, "dead-air" loses the attention of the audience. When attention and credibility are lost, adversarial messaging has the opportunity to fill the void and change the subject or meaning surrounding events and issues. This does not mean to so overwhelm an audience with nuisance "chatter" but to keep their interest with relevant and culturally nuanced information.

Think of messaging as conversational. We all know people who talk at us with little to say and whom we avoid or "tune-out". We also all know people who we can listen to for extended periods of time because they have information and ideas worthy of our attention. The bottom line is that we must be worthy of holding an audience's attention by being credible and talking with rather than talking at them. Sustained messaging across the spectrum of strategic, operational and tactical (local) requires infrastructure and C2 (Command and Control) capable of managing information flow. I will return to this critical issue in depth, later in this article.

A comprehensive communication strategy which can hold the attention of an audience and exert predictable influence includes messaging which supports and is woven into a narrative strategy. A glaring inadequacy of USG/ DoD messaging is the doctrinal addiction the old adage of "themes and messages". Themes and messages as an effective, self-contained communication strategy are a false premise. **While the themes and messages are important, they are sub-components of narrative**. Themes are the story-line of a narrative which give it meaning. Messages merely reinforce those themes. Think of themes and messages as a body walking with legs and arms flailing but headless. This is themes and messages without narrative. Narrative is the missing head that tells the arms and legs where they're going and explains why.

Every action taken in support of USG intentions is a messaging opportunity, good or bad. **Remember, narrative is about identity and co-creating identity between narrator and audience**. Even messaging around a difficult or negative issue is an opportunity to further the bond between narrator and audience. For example, the issue of collateral damage in Afghanistan by US or NATO forces was at one time so critical that such an event would shut-down operations until the matter could be resolved. Becoming proactive, controlling the narrative with honest and immediate reporting reversed this dynamic nearly 100% of the time. Actions must be taken with narrative and messaging support considered.

Another gross inadequacy of messaging is that the USG, specifically DoD is narrowly focused on specific capabilities or in civilian terms tools, when it comes to influence operations. Only a couple of these tools are considered messengers. This could hardly be further from the most effective messaging architecture. As I learned my trade as an IO (Information Operations) practitioner, I learned early on that anyone, any entity or any action impacting my target audience was a "messaging opportunity". It is not only the USG or the US military that comes into contact with audiences important to what Russia is doing. Nearly every agency within the USG, private companies, NGOs, private citizens etc. all are in contact with relevant target audiences. Every single one can and should be considered a part of the influence puzzle. Russia and other adversaries understand this very well and employ this strategy against us with startlingly effective results. Ignoring this aspect by antiquated adherence to doctrine is precisely analogous to fighting with one or both hands tied behind our back.

No focus on messaging would be complete without calling out one of our most glaring discrepancies; lack of cultural nuance in messaging. For a nation of immigrants our messaging is painfully devoid of cultural nuance. This is not just in regard to the message per se but also in regard to the delivery methods and messengers. Again, in regard to narrative, the issue of identity is key. Cultural nuance that addresses specific identity is the bond created between narrator (messenger) and audience.

The bottom line to a messaging strategy is that analysis, integration, and command & control that are both visionary and responsive are critical. Russian influence operations operate with this axiom. Interestingly enough, Russian strategy regarding influence shares a great deal in common with ours. The primary difference though is that Russia actually employs, assesses and recalibrates for more effectiveness. Yes, there is much hand-wringing within USG/ DoD circles regarding oversight, authorities and integration but hand-wringing, think-tanking and failure to execute across the spectrum of the USG still hobble US efforts.

Recommendations:

- Create, staff and authorize tasking authority to a single USG entity charged with developing, disseminating and assessing strategic communications and supporting narratives/messaging
    - **Above all, provide this entity with funding, resources, tasking authorities and legal authorities**
- This single entity would be civilian lead with a board comprised of senior leaders from DoD, DoS and all other relevant entities including the Intelligence Community.
- Create a comprehensive narrative strategy that includes a FoNs (family of narratives) that can create narratives which speak to multiple and disparate audiences, friendly, adversarial and uncommitted.
- Designate a core analysis community of IC professionals that can track, analyze and assess dissemination of narratives and supporting messaging.
- Create a digital TF (task force) with innovative and current technology that collects, analyzes and assesses dissemination friendly and adversarial.
- Create a sub-component that synchronizes a US narrative/ communications strategy with friendly nations and non-state entities.
- Ensure that a comprehensive approach to messaging can be achieved to accommodate long and short term (responsive) messaging requirements.
- Integrate dissemination stake-holders into this entity.
- Ensure all current stakeholders within the USG are represented while concurrently eliminating the current plethora of layered working groups that are bureaucratically prohibitive.

V. Demonstrate by actions that aggression will be firmly resisted

As previously noted, Russia is much the schoolyard bully, albeit far more dangerous. Firm, unrelenting and well explained deterrence, including painful consequences are currently the best option for slowing Russian aggression. Strong deterrence only buys what the US military calls “white space”. It would allow us to catch our breath, form/execute a strategy that includes the 5 recommended courses of action in this article. There are many forms of deterrence and they all need to be explored in support of delivering the most balanced and proportionate response. The recent sanctions on nineteen Russian individuals and entities are valuable. CYBER deterrence is valuable in that it demonstrates to Russia that “living by the sword means dying by the sword”. Again, the paradigm of proportionality is key. We’re not looking for war but stability that is sustainable and secure. This concept is very much the same as Cold War MAD (mutually assured destruction) concepts.

Regardless of the type of deterrence employed, it could hardly be more important that both Russia and our Allies clearly understand our intent, resolve and depth in deploying deterrence. Narrative is the only means by which effective communication of who we are and what we intend can be delivered.

Every theme and message regarding deterrence must be tied to our overarching narrative about who we are and what we will stand for or not. Every PR regarding our actions, every action taken and every ramification of our actions in regard to our Allies must be explained by way of narrative principles so that we are not misunderstood and so that we do not edge closer to open conflict. Deterrence, above all else is a message and must be delivered with all the nuance and sensitivity of any effective messaging.

All historians well remember the lessons of “The Guns of August”, when actions and messages caused catastrophic miscalculation and all-out war in 1914. Nuanced strategy, narrative-centric messaging and carefully proportionate actions (also messages) reinforce order, stability and mitigate the most dangerous aspects of brinkmanship.

Deterrence, like all components of influence operations requires exacting and detailed analysis which demands innovation in what we collect and how we analyze and synthesize collection. Human terrain analysis, including in the digital realm currently is not a specialty of US and many Western Allies. All influence requires “knowing your adversary”. Narrative identity analysis as an example, requires psycho-cultural analysis which is far more exacting than what can be provided in scale by our current intelligence disciplines. In short, what works for deterrence in regard to one target group or state, very likely will not be as effective in other groups. Deterrence tailored to a specific target group is the key to proportionate and effective deterrence.

Recommendations:

- Integrate all action & deterrence with coordinating messaging along with the recommended messaging entity in order to shape cognitive environments and fully exploit all deterrent actions as they occur.
- Though it is implied, it is critical to understand that deterrence measures taken in the CYBER realm must be integrated with all other messaging elements rather than operating in isolation from all other influence efforts.
- Pre and post activity assess the effects of deterrence measures as to risk along with pre-planned contingency actions.
- Pre and post coordinate with affected state and non-state partners likely to be impacted by such measures.

Putting it all together

As with any strategy, it is not the individual elements alone that matter. While each of the five components of this recommendation are critical to the whole strategy, they are not stand-alone. None will achieve significant results in the absence of employing all five to their fullest effect, choreographed within the parameters of overall strategy.

In order to achieve the most positive results these five components must be managed by a single entity with tasking authority over the dozens of entities within the USG that hold sway over the relevant pieces. This will mean that those myriad elements give up some control over their assets in order to contribute to the whole. In our current national security architecture, this is asking a great deal, mostly due to budget issues in which each element fears co-mingling their budgets. In order to overcome this and related hurdles it will require firm and visionary leadership by the senior leaders of all these agencies, entities, and programs. This also by default will require the IC to break down the institutional barriers of cooperation long seen as prohibitive. Again, if leadership wants to achieve greater results, they will need to force the requisite evolution.

During the Cold War, the US managed the C2 of such activity largely by way of the now defunct USIA (US Information Agency). We disbanded this agency in the late 1990s and are now paying the price. Also, OSD/DoD in the 2011/ 2012 time-frame did away with Strategic Communications. What has been left in their place is a hodgepodge of informal and ineffective collaboration which is more personality dependent than a well-oiled and tuned machine of influence. IO (Information Operations) in theory should coordinate such activities for DoD but for reasons too many to articulate, they here have failed miserably. To be blunt, US leadership responsible for influence activities can no longer afford to merely tinker with the antiquated machinery of influence but immediately undertake radical surgery to rid ourselves of the cancer of bureaucratic protectionism afflicting the US national security community.

As noted under the topic of resiliency, this must become a high priority which underlies much of the other 4 components of the strategy. This is a generational problem at best. As with all long roads, the first step is the hardest. The advantage though is that it is ultimately, the least resource intensive by comparison. Leadership that empowers creative thinking within their organisations to insist on factual, in-context information is critical. Also, their “lead by example” requirement sets the tone for their organisations. In a hyper political information environment, this may be difficult but should leaders of opposing political persuasions demonstrate courage, it is achievable.

With a “hardened” information target audience (s) an immediate improvement can be realized. CYBER has a big role in supporting resiliency. Technology which identifies content, outlets and automated SM, while simultaneously neutralizing divisive content takes the pressure off of audiences all too ready to retreat into their ideological corners.

Offensive CYBER also can and must simultaneously demonstrate through deterrent actions that continued efforts to divide and target US & Allied audiences and infrastructure will not be tolerated. Defensive CYBER can contribute greatly to protecting the data of individuals and organisations which further reduces the hypersensitivity within targeted audiences. Many of the tools exist and must be employed with far fewer prohibitive hand-wringing sessions from those in charge of such tools.

Messaging, messaging and more messaging which is synchronized by a single entity could hardly be more important. For a nation with one of the most capable communication and media communities in existence, we fall miserably short when communicating with the rest of the world in support of our intentions. Like everything within the US government, messaging has become so disjointed, bureaucratic and stove-piped as to be nearly ineffective. One of our most glaring shortcomings is that in a nearly instantaneous information environment, we have a miniscule fraction of the capability to message in a timely fashion. This could hardly be truer than in military environments and especially in regard to coordinating with the rest of the USG. Again, this is a simple fix when applying common-sense supported by visionary leadership, but in our current architecture nearly unachievable for the previously discussed reasons.

Finally, and coming full circle to the beginning point regarding "narrative warfare", we have zero narrative strategy. Virtually every one of the five components of this strategy are based on our intent as a nation. Without communicating who we are, what is the meaning of our actions (or not) in a form that relates our identity to that of our audiences, we will continue to fail. To punctuate this point, I cannot count the times that in conversations with friend and foe alike I have been asked, why is the US doing this or that? What do your actions and messages mean? If we cannot answer these basic questions, we have allowed our adversaries to control the narrative of our actions. Currently, Russia dominates the meaning of US and Allied actions with a "the West is threatening mother Russia and we are merely protecting ourselves with the resources available" narrative. Rebutting this requires that we dominate the narrative space and as we all can see, sporadic and random press releases of rebuttal simply won't do.

So, here's the bottom line: Let's tell our story so that everyone understands it. Let's protect ourselves from adversarial stories and related content. Let's clearly demonstrate to our adversaries that there is a price to pay for their aggression and ultimately, let's make our story worthy of all audiences.

Summary

The simplest reason that there are only five recommended courses of action discussed in this paper is that we are currently in crisis mode. In short, we must take action and soon. By all estimations, the ability to develop, resource and staff a competent influence organisation is prohibitive in a short period of time. Implementing the basic five-pronged approach with available/re-tasked resources, though daunting in scope and as described in this paper, is still pragmatically streamlined in comparison. The bottom line is that in order to adopt any strategy, short or grand in scale, we must break from decades old national doctrine. Yes, old habits are hard to break… but not impossible.

The take-a-way lesson to this entire discussion regarding an influence strategy for Russia is that in order for any of these recommendations to become effective, we must have an entity which can strategize, coordinate and execute influence. We can no longer afford to hope for successful long-term collaboration without leadership, training, resources, legal authorities and divorcing ourselves from the plodding, protectionist bureaucracy which currently satiates the USG national security community. The latest US DoD budget of $700 plus billion dollars including a windfall of $61 billion in additional funds shows that influence has been nearly ignored. When every reasonable and credible defense analyst is declaring that **conflict beneath the threshold of all-out war is the new norm,** the logic for focusing on bombers, ships and tanks is fatally flawed. Common sense dictates that prioritized planning for threats needs to be based on analysis, not the bottom line of big defense contractors. Our current analysis says clearly, that conflicts are now influence-centric and so by default, common sense requires prioritizing resources in a manner that meets the needs of regaining influence dominance.

As noted in the aforementioned sports analogy of football; we cannot compete without all the players, a playbook, training, support staff, recruiting, innovation and the requisite resources for everyone from the water-boy to the coach. The coach also must have control of the entire apparatus who can make the necessary adjustments as the game evolves. Anything less results in regular and routine failure. This failure is precisely what we now are experiencing.

Finally, a reminder that *"Influence done well is a complex and intricate choreography of actions, words and related activities".* Just the bare minimum requirements and related discussion have fully filled the preceding pages, with far too much still unsaid. I have little doubt that there will be firm and detailed resistance from many of the communities now charged with the tasks of influence and I welcome it. Intense and detailed professional discussion is required for problem solving. Action, resulting from those discussions is even more important. If this paper encourages and prompts such action, even in the face of criticism, it will have been worth the effort. A reminder to those that would challenge me; as with the quote at the very beginning of this paper; "don't just complain, present solutions

About the author

*Paul Cobaugh is a retired US Army Warrant Officer that spent the last 15 years of his career as an IO (Information Operations) practitioner in the US Special Operations community with multiple deployments to combat zones. For the past two years he has served as Vice President at **Narrative Strategies**, a US-centric think & do tank dedicated to supporting national security objectives through non-kinetic influence.*

Bibliography

Association, A. P. (n.d.). *The road to resilience*. Retrieved from http://www.apa.org/helpcenter/road-resilience.aspx

Berk, A. W. (n.d.). *The Strategic Communication Ricochet: Planning Ahead for Greater Resiliency*. Retrieved from The Strategy Bridge: https://thestrategybridge.org/the-bridge/2018/3/7/the-strategic-communication-ricochet-planning-ahead-for-greater-resiliency

Bertolin, G. (2017, November). *Digital Hydra: Security Implications of False Information Online*. Retrieved from STRATCOM COE: https://www.stratcomcoe.org/digital-hydra-security-implications-false-information-online

Clark, D. H. (2017). *Information Warfare, the lost tradecraft.* Narrative Strategies, LLC.

Cobaugh, C.-a. P. (2017). *Soft Power on Hard Problems.* Hamilton Publishing.

Cobaugh, P. (2017, August 12th). *Who we are as a nation*. Retrieved from Medium: https://medium.com/@paulcobaugh/these-days-you-might-say-that-story-telling-or-narrative-is-my-trade-79aaf1acfa9f

Cobaugh, P. (2018, February 27). *Narrative primer for understanding the power of narrative as the core tool of influence.* Retrieved from Medium: https://medium.com/@paulcobaugh/narrative-primer-for-understanding-the-power-of-narrative-as-the-core-tool-of-influence-c6710f4a2553

Cobaugh, P. (n.d.). *It's not just social mdia*. Retrieved from Medium: https://medium.com/@paulcobaugh/influence-is-not-just-sm-c675d33ca970

Cobaugh, P. (n.d.). *Narrative primer for understanding the power of narrative as the core tool of influence*. Retrieved from Medium: https://medium.com/@paulcobaugh/narrative-primer-for-understanding-the-power-of-narrative-as-the-core-tool-of-influence-c6710f4a2553

David A. Shlapak, M. J. (2016). *Reinforcing Deterrence on NATO's Eastern Flank*. Retrieved from RAND: https://www.rand.org/pubs/research_reports/RR1253.html

Emmott, R. (n.d.). *NATO mulls 'offensive defense' with cyber warfare rules*. Retrieved from Rueters: https://www.reuters.com/article/us-nato-cyber/nato-mulls-offensive-defense-with-cyber-warfare-rules-idUSKBN1DU1G4

Erika Manczak, i. a. (2015, August). *Life's Stories*. Retrieved from The Atlantic: https://www.theatlantic.com/health/archive/2015/08/life-stories-narrative-psychology-redemption-mental-health/400796/

Fridman, O. (2017, Spring). *STRATCOM COE publications* . Retrieved from STRATCOM COE: https://www.stratcomcoe.org/ofer-fridman-russian-perspectiveon-information-warfare-conceptual-roots-and-politicisation-russian

Fundamentals of Cyber Conflict. (2017, May). Retrieved from Stanford University: https://seclab.stanford.edu/courses/cs203/lectures/lin.pdf

Green, E. (2017, March 16). *'Distracted and distractible': The rise of propaganda*. Retrieved from Streetrootsnews: http://news.streetroots.org/2017/03/16/distracted-and-distractible-rise-propaganda

Hermann, J. (2018, April 5). *Defense and Self-Defense in the Information Age: Collaborative Strategy and Collective Vision*. Retrieved from The Strategy Bridge: https://thestrategybridge.org/the-bridge/2018/4/5/defense-and-self-defense-in-the-information-age-collaborative-strategy-and-collective-vision

Information Operations. (Routinely updated and current). Retrieved from Cyberspace and Information Operations study center: http://www.au.af.mil/info-ops/what.htm

John Cook, S. L. (2017, May). *Neutralizing misinformation through inoculation: Exposing misleading argumentation techniques reduces their influence*. Retrieved from PLOS: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0175799

Lewis, E. F. (2017, Oct). *A Right-Brained Approach to Critical Infrastructure Protection Theory in support of Strategy and Education: Deterrence, Networks, Resilience, and "Antifragility"*. Retrieved from NPS HOMELAND SECURITY AFFAIRS: https://www.hsaj.org/articles/14087

Lydia Kostopoulos, P. (2017, November 14th). Retrieved from LYDIA KOSTOPOULOS, PHD @LKCYBER: https://www.slideshare.net/lkcyber

Lydia Kostopoulos, P. (2018, April 3-6). Cyber Military Education in an Era of Change NATO presentation. Japan. Retrieved from (NEED URL HERE)

Maan, D. A. (2009). *Internarrative Identity: Placing the Self.* UPA.

Maan, D. A. (2010). *Internarrative Identity: Placing the Self.* Lanham, Md. : University Press of America.

Maan, D. A. (2015). *Professor/ Author Counter-Terrorism Narrative Strategies .* University Press.

Maan, D. A. (2018, February 27). *Narrative Warfare*. Retrieved from Real Clear Defense: https://www.realcleardefense.com/articles/2018/02/27/narrative_warfare_113118.html

Maisel, W. D. (2017, August 15). *It's Time to Bring Back This Cold War Agency and Stop Ceding the Propaganda War to Russia*. Retrieved from Modern War Institute at West Point: https://mwi.usma.edu/time-bring-back-cold-war-agency-stop-ceding-propaganda-war-russia/

Malcher, A. (2015, May 10). *Russian Spetsnaz – Ukraine's Deniable 'Little Green Men'*. Retrieved from Modern Diplomacy: https://moderndiplomacy.eu/2015/05/10/russian-spetsnaz-ukraine-s-deniable-little-green-men/

McAdams. (2015, August). *Life's Stories*. Retrieved from The Atlantic : https://www.theatlantic.com/health/archive/2015/08/life-stories-narrative-psychology-redemption-mental-health/400796/

McClintock, B. (2017, July 21). *Russian Information Warfare: A Reality That Needs a Response*. Retrieved from RAND: https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html

Monisha Pasupathi, a. p. (2015, August). Professor of developmental psychology at the University of Utah. *The Atlantic*.

Multiple. (2018, March 12). *Final report of the High Level Expert Group on Fake News and Online Disinformation*. Retrieved from https://ec.europa.eu: https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

Pentagon drops 'strategic communication'. (2012, December 3rd). Retrieved from USA Today: https://www.usatoday.com/story/news/nation/2012/12/03/pentagon-trims-strategic-communication/1743485/

Polyakova, A. (2018, March 20). *The Next Russian Attack Will Be Far Worse than Bots and Trolls*. Retrieved from The Lawfare blog: https://lawfareblog.com/next-russian-attack-will-be-far-worse-bots-and-trolls

Sallanpaa, A. (2016, October). *kremlin-and-daesh-information-activities*. Retrieved from STRATCOM COE: https://www.stratcomcoe.org/kremlin-and-daesh-information-activities

The Epic Identity of the Iliad and Odyssey: Pindar and Herodotus' Lofty Legacy. (n.d.). Retrieved from Center for Hellenic Studies, Harvard University: https://chs.harvard.edu/CHS/article/display/5857

Todd C. Helmus, E. B.-B. (2018, April 21). *Russian Social Media Influence*. Retrieved from RAND: https://www.rand.org/pubs/research_reports/RR2237.html

US Information Agency. (n.d.). Retrieved from This web site is an archive of the former USIA site as it stood in September 1999, and is now maintained as part of the Electronic Research Collection of historic State Department materials by the federal depository library at the University of Illinois a: http://dosfan.lib.uic.edu/usia/

Weaponized Narrative Initiative. (2018). Retrieved from Weaponized Narrative Initiative at Arizona State University: https://weaponizednarrative.asu.edu/