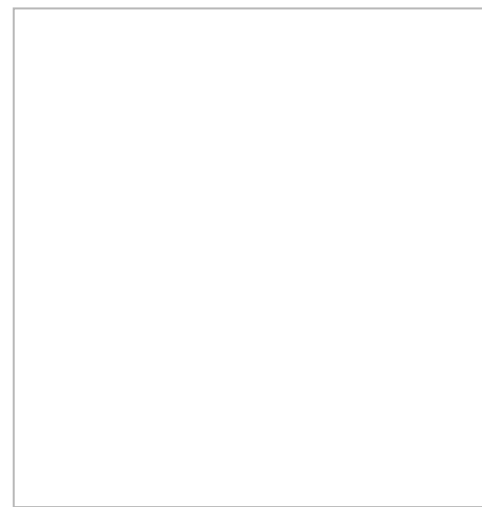
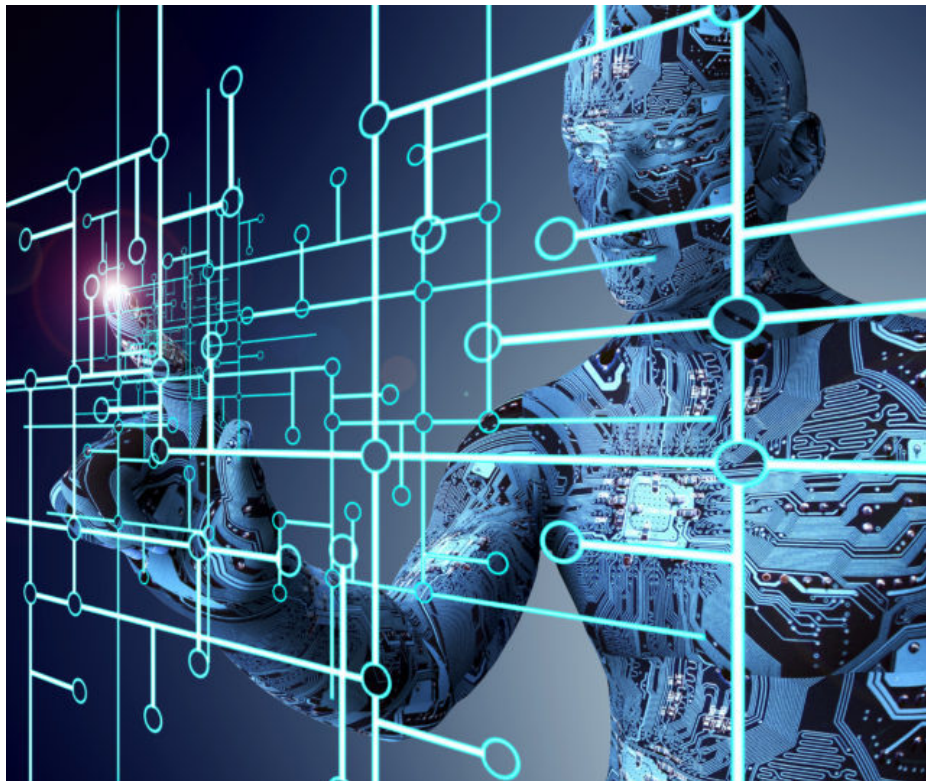




Narrative, Cyberspace and the 21st Century Art of War

Posted on January 22, 2017 by Brad D. Williams



Sign up to get the top Fifth Domain new
Daily Brief:

Email Address

SUBSC. ^

In February 2015, an article insipidly entitled “[The Value of Science in Prediction](#)” appeared in the Russian publication *Military-Industrial Courier*. The article was penned by Valery Gerasimov, chief of the general staff of the Russian Federation. Few in the West recognized the article at all, much less its significance, at the time of its publication.

In the article, Gerasimov analyzed “new-type conflicts.” These conflicts entail an array of strategies and tactics employed in the [gray zone](#) to achieve national interests, even military, without a declaration of war and without crossing the threshold that would provoke a kinetic response.

“The very ‘rules of war’ have changed,” Gerasimov wrote.

Dr. Mark Galeotti, an expert on Russian history and security issues who [annotated](#) an English translation of Gerasimov’s article, identified the most important line as, “The role of nonmilitary means of achieving political and strategic goals has grown and, in many cases, they have



Norms aren’t substitute for international law in cyberspace



33M government, corporate employee records leaked from DUNS database



Hackers shut down Swedish military exercise systems



Cyber ops need common lexicon to align with war domains, say analysts

Gerasimov's "nonmilitary means" included "broad use of political, economic, informational, humanitarian and other nonmilitary measures – applied with the protest potential of the population."

Experts see one hybrid tactic – narrative and cyber – playing an increasingly prominent role in current conflicts.

War Narratives

An old Wall Street adage goes, "You'd have to be a paranoid Russian poet to understand global finance." Today, that maxim might be paraphrased for an equally unexpected insight: "It helps to be a literary critic in understanding contemporary warfare."

In *The Art of War*, Sun Tzu described the "five constant factors" of conventional warfare, but none included narrative. Experts now point to the influential role of narrative in military, geopolitical and ideological "new-type conflicts."

audiences, advance agendas and engage adversaries.

Scholars have long argued that literary techniques are not the special purview of novelists, poets and playwrights. From philosophers' research on [metaphor](#) to cognitive scientists' investigations into [parable](#), literary devices reveal and appeal to basic human cognition. Perhaps that's why narrative's use by governments, institutions, businesses and ideologues is not new.

When employed in military or geopolitical conflicts, Brad Allenby and Joel Garreau, co-directors of The Weaponized Narrative Initiative of the Center on the Future of War, call it "weaponized narrative." And they believe its recent effectiveness will encourage further use.

In an email interview, Allenby said, "Weaponized narrative is not a temporary or passing phenomenon. It is based on significant recent advances in science, technology and social use of technology."

Conflict Resolution and CEO of Narrative

Strategies, notes that narrative's power precedes technology.

In an email interview with Fifth Domain, Maan said:

Advanced technologies work to disseminate messages farther and wider than they would be otherwise, but narratives are already there, on the ground, in people's heads. The enemies of the U.S. and her allies understand this very well. Advanced technology is a tool. The center of gravity is the narrative.

The "Era of Cybered Conflict"

Current conflicts play out, at least partly, in cyberspace.

Dr. Chris C. Demchak, RDML Grace Murray Hopper professor of cybersecurity and director of the Center for Cyber Conflict Studies at the U.S. Naval War College, characterizes today's environment as one of "cybered conflict."

Due to the massively insecure technology of the global cyberspace, we in the West have created a widely spread, poorly secured cyberspace “substrate” that allows attackers in any numbers, from anywhere, with any tools and for any reason to cheaply reach into our critical systems with minimal chances of being punished. The result is that the world has been thrust into an era of “cybered conflict.”

Like Gerasimov’s blurred line between war and peace, Demchak described cybered conflicts as “stretch[ing] from peace through traditional war.” Importantly, Demchak highlighted the strategic advantages of cybered conflict relative to conventional war:

explosively. Rather, it is marked by exceptional advantage to deception in what tools are used and opaqueness in who, in what numbers, are using them. Going to the end of the spectrum – to “cyberwar” – is relatively inefficient and opens oneself up to direct retaliation throughout one’s own societal systems. Instead, one can slowly demolish an opponent without ever killing someone or destroying something with a kinetic tool traceable back to oneself ... [which] is much safer, reliable and easier to outsource.

Russia, China and ISIS are all leveraging the advantages afforded by cybered conflict to employ hybrid warfare tactics – from hacking to weaponized narrative.

Russia and the Grand Nationalist Narrative

Russia’s use of hybrid warfare long predates Gerasimov’s article. Noting the Soviet Union’s traditional outward posture since the Cold War’s advent, Demchak said, “Russia innovated the strategy of disinformation and personalized

Allenby noted favorable conditions for disinformation persist today: “The Russian system tends to reward the cynical, morally relativistic psychology that best aligns with developing and deploying weaponized narratives.”

As foreshadowed by Gerasimov, Russia has displayed its hybrid capabilities during the Ukraine conflict. Allenby points to Russia resurrecting the historical “[Novorossiya](#)” and adopting the newer “[Russian Eurasian Empire](#)” narratives.

Such narratives matter, Allenby explained, “Because suborning an adversary through weaponized narrative is far, far less costly than a conventional attack. Weaponized narrative offered an important way to achieve Russian ends while not justifying a conventional response under the UN charter.”

Allenby also noted the hybrid approach, which included narrative and “fomenting insurrection

Allenby added, “Was the invasion [of Crimea] effective? Absolutely. Was it a strategic success? For that, we’ll have to wait and see.”

Asked about the similarities and differences between Russia’s tactics in Ukraine and the [alleged activities](#) carried out during the 2016 U.S. presidential election, Allenby said:

The two are similar, in that causing a degree of confusion and social fragmentation in the target is a major strategic goal. The tools are different because the cultures are very different, and the follow through is different ... Nonetheless, the underlying processes, operations and design of weaponized narrative campaigns must be similar because they are based on the same advanced science, new technologies and rapidly evolving understanding of human psychology.

China and the Sovereignty Narrative

China is also using narrative to further its geopolitical agenda. China’s interest in expanding territorial sovereignty in the South China Seas is

At issue is, Demchak wrote, “China wants her borders in cyberspace and will take nothing less.” Whereas the West sees the internet as a tool for global democratization, “the Chinese narrative accentuates the instability and greater dissent that can accrue with a border-spanning open internet.”

China’s view implicitly acknowledges Gerasimov’s “protest potential of the population.”

To achieve cyber sovereignty, China has employed hybrid gray-zone tactics.

“China,” Demchak wrote, “is also hoping to hurry along the [U.S.’s] apparent decline with narratives, money and stealth and yet control the narrative of a no-threat peaceful rise well enough to stay short of physical conflict.”

China’s cyber sovereignty is part of a grander narrative. “China justifies its rise in the world – its ‘rightful place’ – on the basis of its population,” Demchak said. “China will not over time tolerate

ISIS and the Narrative of the Islamic Caliphate

The rise of ISIS surprised many in the West. Narrative and cyberspace played a central role, experts say.

Counterterrorism scholars have studied the “messaging and counter-messaging” of ISIS. Maan thinks ISIS’s narratives are more “profound and pervasive” than simple messaging.

“It is through narrative that identity is constructed: Personal identity, communal/clan identity and national identity,” she said. “It is formative in the identity layers of all parties to communication long before any communication has taken place between them.”

In her writing, Maan has examined a common [idea](#) across ISIS’s communications: “Islam is under attack.” That is a [title](#), not the narrative, she explained.

Despite the West’s claims otherwise, “Islam is under attack” resonates with ISIS followers in

events.”

Maan argues, rather than focusing on counter-narrative, which oftentimes “emboldens” the original, the West should develop its own. To succeed, Maan thinks the West’s narratives must be credible and based on the “production of common sense.”

“That is how successful narratives appear. They don’t seem like a construction. They seem to reflect ‘just the way things are,’” she said.

Previous

Next

◀ Cyberattack on Sundance

China Cracks Down on Tools ▶

Briefly Shuttters Box Office

Used to Get Around Web Filters

FIFTH DOMAIN
CYBER



Civilian

DHS
FBI/DOJ
OMB

DoD
Air Force


Critical
Infrastru
cture

Internati
onal

Services

- About Us
- Advertise with Us
- Contact Us
- Privacy Policy
- Terms of Service



 Search ...