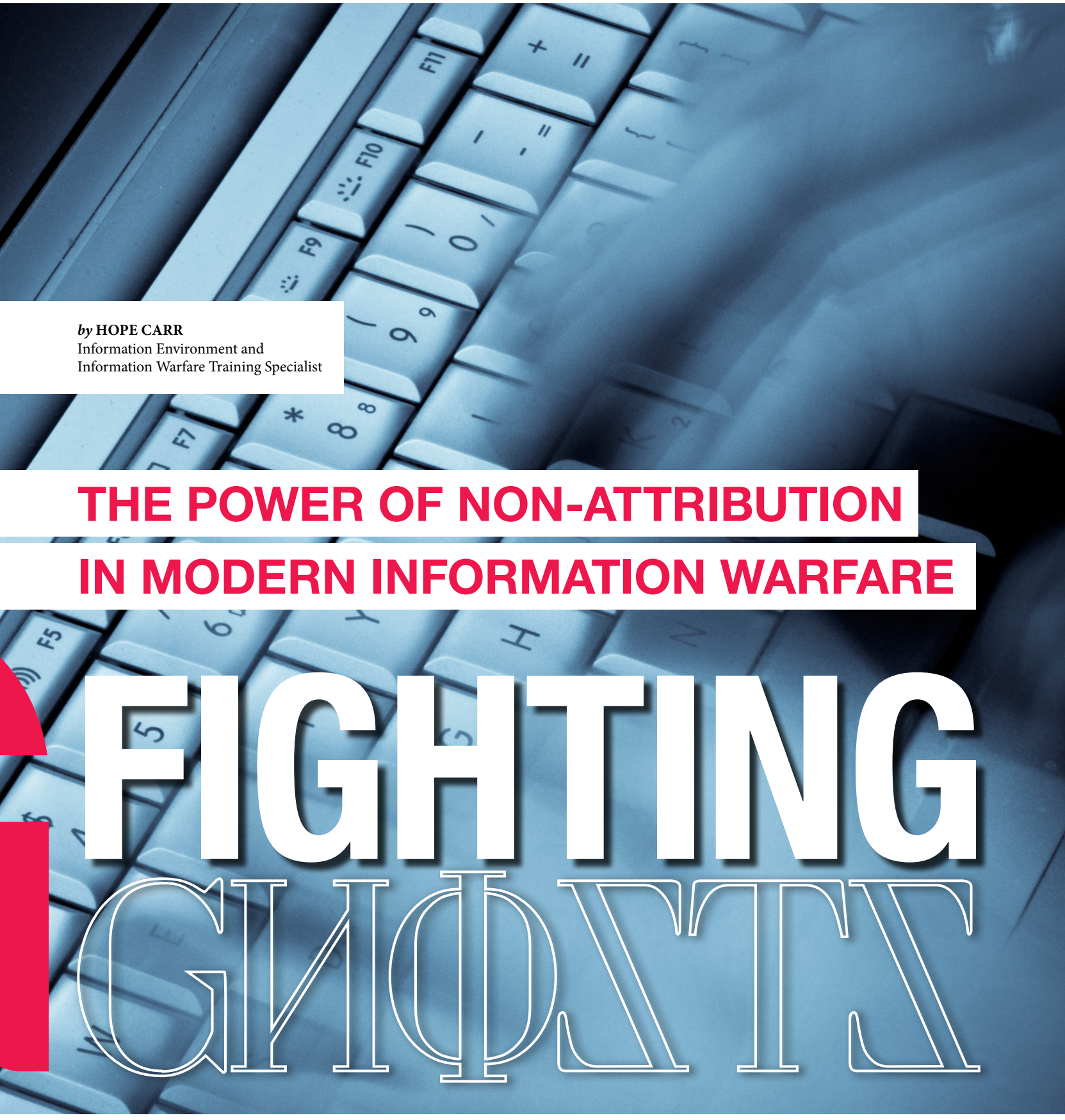


by **HOPE CARR**
Information Environment and
Information Warfare Training Specialist

THE POWER OF NON-ATTRIBUTION IN MODERN INFORMATION WARFARE

FIGHTING

"The approach is guerrilla, and waged on all fronts with a range of actors and tools—for example, hackers, media, businessmen, leaks and, yes, fake news, as well as conventional and asymmetric military means. Thanks to the internet and social media, the kinds of operations Soviet PSYOPS teams once could only fantasize about, upending the domestic affairs of nations with information alone, are now plausible."

Molly K. McKew
Politico Magazine, September/October 2017

Retrace your steps since you woke up this morning. What was the moment that the external world began to influence your perception? When was it that you reached into the cyber domain to inform your day? For me, it was 5:15 a.m. I woke up at 5:00 a.m. and was sitting with my smartphone looking at the top morning headlines just 15 minutes later. Some of you may make it a little bit longer than I did, but I would guess the majority are flipping through feeds, websites, social media and all of the comments that accompany them within a few hours of getting out of bed. Further, when we make it to where we are around actual people, we quickly fall into the habit of talking and discussing things we have read, heard or saw. Those topics with the most likes, shares or comments are often driven to the top of the feeds, websites and social media platforms that we go to, and as a result, are often the shared topics we discuss throughout the day. All of this is shaping the way we perceive events, ideas and the world around us.

While this is not so different from before when we relied on more traditional mediums like radio, newspapers and television, the speed, amount of content, and the deliverers of information are. We have all seen it happen. A rumour grows into comments, then into a trending topic, then branches out into articles, TV and radio, often without a single idea of where it sprouted from or why. In an attempt to just keep up with all of the information out there, the questions of *WHO* and *WHY* often get pushed to the back burner and the power of volume becomes the validator for authenticity and trustworthiness. But, the *WHO* and *WHY* are the critical questions everyone should be asking in today's information saturated world.

Information environment and modern warfare

This pattern is not just limited to our social lives or our morning headlines. Today, the influence of information and attribution has pushed into diplomacy, politics and military operations. If you Google© "information and warfare", it brings up over 138 million hits in just .62 seconds. This number is expected to grow as the concept of information warfare, "fake news" and "alternative facts" becomes even more entrenched in our daily lexicon.

While the role of information warfare has long been discussed within military organisations, the public consumption of the concept truly began following Russia's November 2014 occupation of Crimea under the guise of "little green men" that allowed Russia to hide in plain sight. As one Guardian article described, after the occupation, "Crimea, a peninsula with many ethnic Russians, is suddenly full of Russian plated-trucks and aircraft, and its parliament and airport seized by men carrying Russian guns, denying that they are Russian."[1]

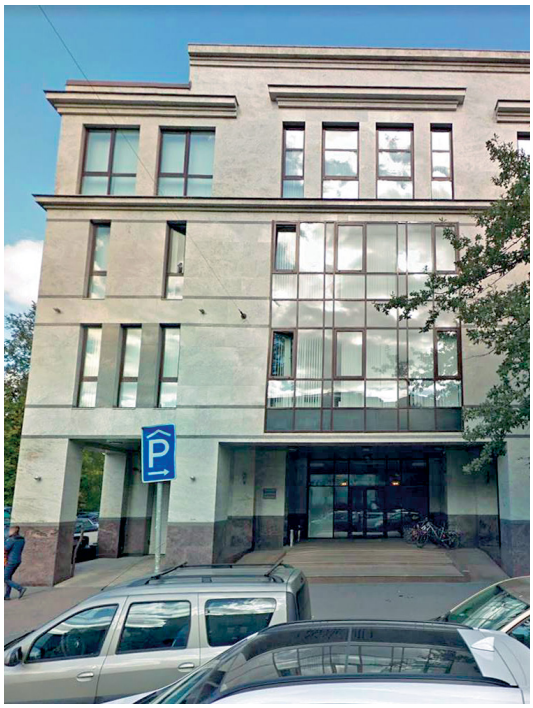
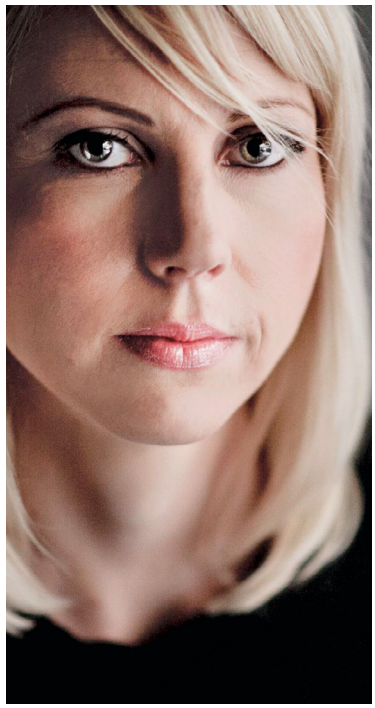
Crucial to this approach was Russia's absolute saturation of the information environment with its own version of reality around Crimea. A 2015 analysis of Russia's information campaign against Ukraine by NATO's Strategic Communications (StratCom) Centre of Excellence (CoE) suggests that "the information campaign and related military action by Russia corresponds to the characteristics of a new form of warfare where the lines between peace and war, foreign military force, and local self-defence groups are blurred and the main battlespace has moved from physical ground to the hearts and minds of the populations in question."[2]

The study identified deception as a critical component of the Russian information warfare strategy "to distract and delay". The CoE stressed that "investigating and disproving the false information, different versions of events and even conspiracy theories rapidly disseminated by Russia requires a lot of time, effort and resources on the part of international organisations like NATO, the Ukrainian government, independent media, experts and even ordinary citizens."[3]

At the heart of this disinformation campaign is the de-centralized distributor. As stated in General Valery Gerasimov, Russia's Chief of the General Staff, published 2013 article, *The Value of Science Is In The Foresight*,[4] chaos is the strategy of choice. As Molly McKrew summarizes in her September 2017 article on the Gerasimov doctrine for Politico Magazine, "Russian intervention is systematic and multi-layered (...) like all guerrilla doctrine, it prioritizes conservation of resources and de-centralization, which makes it harder to detect and follow."[5]

Non-attribution

Non-attribution is a critical piece of the decentralized component of Gerasimov doctrine. Dr Andrew Monaghan, a Senior Research Fellow at Chatham House and a Visiting Fellow at the Changing Character of

ABOVE: Chief of the Russian General Staff, General Valery Gerasimov. In the hierarchy of the Russian government, there are uniformed officers serving in positions technically above the Chief of the General Staff, but arguably none of these assignments are as prestigious. Photo by Free Wind, Shutterstock. **MIDDLE:** The now-defunct Internet Research Agency in St. Petersburg, which was, in fact, a Russian troll factory, with hundreds of workers trained to pump out misinformation online. Photo by NBC News © www.nbcnews.com **RIGHT:** Journalist Jessikka Aro, who became a target for pro-Russia propaganda (http://kioski.yle.fi/). Photo by @jessikkaaro

War Programme, Pembroke College, Oxford, suggests that Russian hybrid warfare "relies on proxies and surrogates to prevent attribution and intent, and to maximize confusion and uncertainty." Conventional force for Russia is seen as supplementary.[6] The InfoSec Institute validates Monaghan's comments calling attribution "a multi-dimensional issue". The Institute suggests attributing content to non-nation-state actors from governments requires multiple source analysis of information, which includes "forensic analysis, human intelligence reports, signals intelligence, history, and geopolitics"; but cautions that "the problem of attribution is exceedingly complex and is not always solvable."[7]

Troll armies, fake stories and corrupt validators

While hackers pose a significant state cyber threat, the greater and less attributable threat may be the ever-expanding troll armies that can flood the online world. These armies, made up of both real people and electronic BOTs, have the power to influence and shape opinions and ideas as we pour over the headlines during our early morning coffees, or read the comments on our morning commute. As Leo Benedicus, an award winner feature writer for the Guardian outlined in his 2016 article *Invasion of the Troll Armies*, "we don't know who they are, or what their mission is. We only know that there are thousands of them out there, pretending to be us."[8]

As the profile of information warfare grows, the public is gaining glimpses into these troll armies. A series of leaks in 2013 and 2014 about Internet Research Agency (IRA) exposed the St. Petersburg based company as a government funded troll army trained and paid to smear Russian opponents. According to documents released by hackers, IRA employed more than 600 people across Russia with an annual budget of $10—$12 million. More than half of the budget was paid out in cash to employees who were expected to post or comment on news articles at least 50 times a day. The documents showed employees with blogs had to maintain six Facebook accounts and publish at least three posts daily or on Twitter, they had to have at least 10 accounts with at least 50 tweets per day. Employees also had targets for both followers and the level of engagement that had to be reached.[9]

In October 2017, CNN broke that IRA, also blamed for interference in the 2017 U.S. elections, was linked to Russian Oligarch Yevgeny Prigozhin a member of Putin's inner circle.[10] IRA has since been shut down.

In another example, New York Times reporter Andrew Higgins outlined the plight of Finnish journalist Jessikka Aro after she tried to expose Russia's troll armies. Aro, a journalist for Finland's national broadcaster, became a personal target for a smear campaign, with the group going so far as to hold a protest against her at the headquarters of Yle Kioski. On the surface this seems small, but the greater impact and purpose goes far beyond attacks on Aro.

Public opinion in Finland is presently deeply divided over Russia, making the nation a target for information warfare. Saara Jantunen, a researcher at the Finnish Defense Forces in Helsinki, says Russia's big concern is to keep Finland out of NATO. To do so, Jantunen says they "fill the information space with so much abuse and conspiracy talk that even sane people start to lose their minds."[11]

Add to this saturation the validation of ideas and narratives by what appear to be credible third parties and the confusion for the consumer only grows. As people become more information savvy, they are doing the second

While hackers pose a significant state cyber threat, the greater and less attributable threat may be the ever-expanding troll armies that can flood the online world.

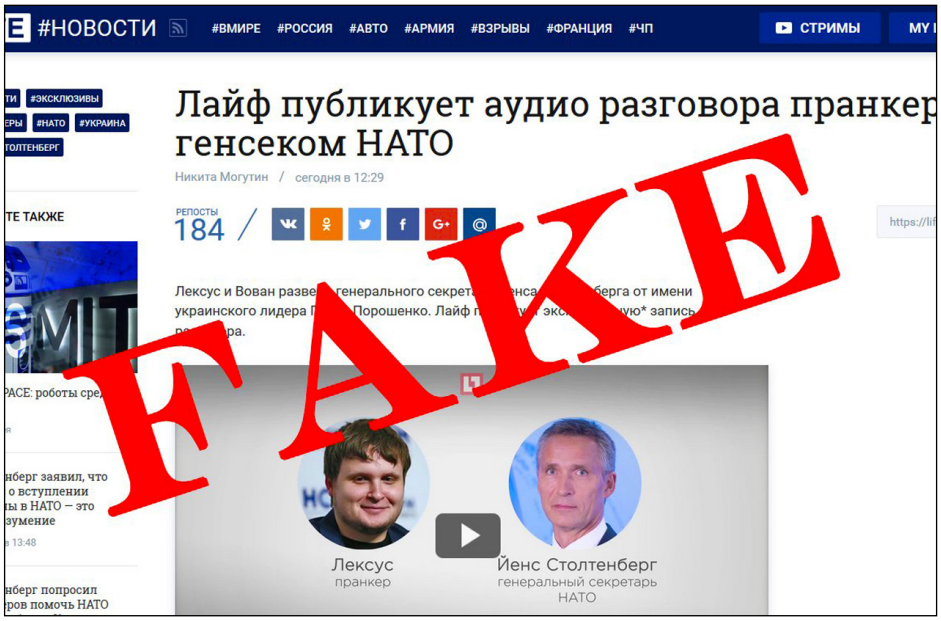
checks to make sure they are not being tricked or influenced but it is not always easy to know what agencies and people are legitimate.

Russian funded non-governmental organizations (NGOs) like the European Research Institute, and think tanks like Global Research in Canada, present doctors, studies and research that are often used to validate Russian narratives, originally driven by trolls and BOTs, once they make it into mainstream media.[12] Linking these organizations and sources to legitimate means of validation means most people are more likely to buy in to the narratives once validated through these third party agencies, which often act as sense-making tools when topics are complex and complicated. Underestimating the power of these tools is what nations like Russia want because the accumulative effect of the comments, shares, likes and saturation of government funded narratives achieved by these troll armies and paid validators shape international opinion and ensure ongoing disruptions and public unrest. The last few years has shown no nation, not even those we once saw as superpowers, are immune from the influence of troll armies and their ability to undermine confidence in once immune institutional safe havens.

We no longer fight soldier-to-soldier

The looming question is "so what" for modern military operations. If we think traditionally about warfare, it would seem that thousands of troll armies in front of laptop or think tanks, NGOs or BOTs will have little effect on the battlefield. But, modern concepts of the battlespace that no longer function within a singular kinetic environment[13] tell a far different story. One that is much closer to that predicted by Marshall McLuhan, the Canadian Godfather of media theory, in his 1970's book *Culture Is Our Business*. McLuhan predicted "World War III [will be] a guerrilla information war with no division between military and civilian participation."[14]

BELOW: The screenshot of the Twitter page of NATO Principal Spokesperson Oana Lungescu countering disinformation in the Russian media and social media space, 3 February 2017. Her message read: "#Russian audio of an alleged call btwn #NATO SG @jensstoltenberg & President @poroshenko is a fake. No such call took place."



The Russian–Finnish border zone. Photo © Thomas Nilsen

Recommended Reading
LESSONS FROM FINLAND

The introduction below is extracted from Dr Katri Pynnöniemi's article, "Hybrid Influence, Lessons from Finland", NATO Review Magazine (2017), www.nato.int

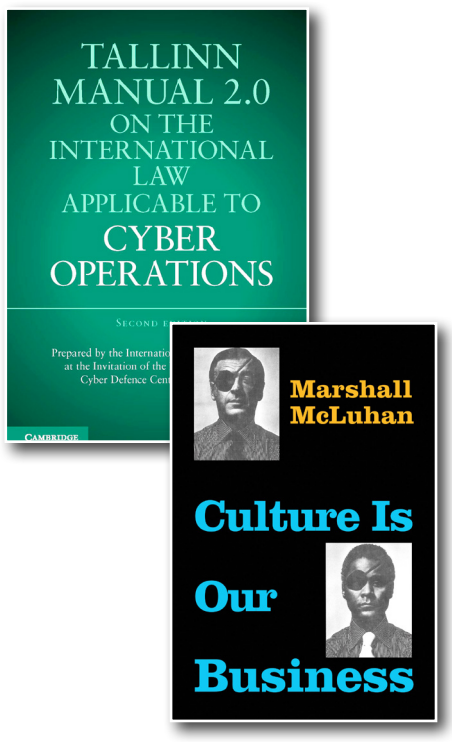
"THE ROOTS OF RUSSIA'S hybrid methods go back to the Soviet era, although the label is more recent. Active Measures, as hybrid was called back then—such as spreading disinformation and setting up front organisations in the West—was an integral part of Soviet foreign policy. Today, some of Russia's tactics are surprisingly similar, but the current information environment makes their use both more efficient and complex.

"As Finland has learned, hostile influence does not always involve pressure tools and 'sticks' but also kind words and 'carrots'. Whether attempts to influence and control the target state are reflexive or coercive depends on the context—but the aims and effects could be similar. Russia's official rhetoric, for instance, offers positive messages of good neighbourly relations, yet on the sidelines, Finland receives reminders that this is not self-evident and that, to maintain good relations, it should behave 'responsibly' (that is, in a way that would not endanger Russia's interests)."

The online article can be found at www.nato.int/docu/review/2017/Also-in-2017/lessons-from-finland-influence-russia-policty-security/EN/index.htm

While time and space have changed the language, Gerasimov expands on McLuhan's prediction and suggests "the information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy."[15] By transcending geography and traditional battlefields, information warfare evens the playing field and renders traditional military superpowers, like the United States, as a peer in the digital battlespace and in the minds of diverse populations.[16] Acting as a force multiplier, troll armies and digital repeaters need no military training, never bear arms, yet significantly impair, influence and shape the battlefields once considered the sole domain of soldiers.

Further, at a cost of just tens of millions of dollars a year for a troll army, nations like Russia are advancing political and social agendas through non-attributed, de-centralized efforts resulting in soft annexation without having to engage in costly traditional warfare. While the amount of money Russia is spending in supporting their vast information warfare machinery is unknown, it is clearly much less sustainable then a costly traditional war. Further, it allows Russia to fund advancements within their traditional military capacities while they continue to effect nationalistic agendas in neighboring nations.



The way ahead for responding to information warfare

The evolution of cyber and electronic warfare, information operations and psychological operations capacities hold promising paths for the world's militaries to respond to non-attribution and information warfare attacks within the frameworks of their own moral compasses. But, just as information warfare has implications beyond military into the political, economic and social, so must the responses to information warfare and non-attribution come from those realms as well.

Bruce McClintock, an adjunct policy analyst at the RAND Corporation and a former U.S. Defense Attaché in Moscow, suggests that "tangible actions" must be taken to ensure unity of purpose in response to information warfare. McClintock suggests the *Tallinn Manual 2.0*,[17] released in February by the NATO Cooperative Cyber Defence Centre of Excellence, is a positive step towards linking international laws that apply to cyber operations but more needs to be done.

McClintock sees the greatest areas for improvement being in common definitions, a clarified position and the linkage of international laws to cyber offenses because only when "laws and norms are binding will there be legal and tangible consequences" for actions within the cyber and information domains.[18] The editors of the *Tallinn Manual 2.0* may have best described the challenge being faced by NATO and other nations as they look forward when they stated: "The Russians are masters at playing the 'gray area' in the law, as they know that this will make it difficult to claim they are violating international law and justifying responses such as countermeasures." ✦

END NOTES:

1 Alan Yuhas and Raya Jalabi. "Ukraine's Revolution and Russia's Occupation of Crimea: How we got here", The Guardian. March 5, 2014. https://www.theguardian.com/world/2014/mar/05/ukraine-russia-explained

2 NATO StratCom Centre of Excellence. "Russia's Information Campaign against Ukraine", 2015. https://www.stratcomcoe.org/download/file/fid/3213

3 Ibid,.

4 Valery Gerasimov. "The Value of Science is in the Foresight", Military Review. January/February 2016. http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf

5 Molly McKrew. "The Gerasimov Doctrine", Politico. September/October 2017. https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538

6 Andrew Monaghan. "The War in Russia's Hybrid Warfare", Chatham House, 2016. http://ssi.armywarcollege.edu/pubs/parameters/issues/Winter_2015-16/9_Monaghan.pdf

7 INFOSEC Institute. "Cyber Warfare from Attribution to Deterrence", 2016. http://resources.infosecinstitute.com/cyber-warfare-from-attribution-to-deterrence/#gref

8 Leo Benedictus. "Invasion of the Troll Armies", The Guardian. November 6, 2016. https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian

9 Ibid,.

10 Tim Lister. "Exclusive: Putin's 'chef', the man behind the troll factory", CNN. October 17, 2017. http://www.cnn.com/2017/10/17/politics/russian-oligarch-putin-chef-troll-factory/index.html

11 Andrew Higgins. "Effort to Expose Russia's 'Troll Army' Draws Vicious Retaliation", New York Times. May 30, 2016. https://www.nytimes.com/2016/05/31/world/europe/russia-finland-nato-trolls.html

12 Wilifred Martins Centre for European Studies. "The Bear in Sheep's Clothing: Russia's Government Funded Organizations in the EU", July 2016. https://www.martenscentre.eu/publications/bear-sheeps-clothing-russias-government-funded-organisations-eu

13 Peter Gizewski and Lieutenant-Colonel Michael Rostek, "Towards a JIMP-Capable Land Force" Canadian Army Journal 10, no. 1 (March 2007): 55-72.

14 Marshal McLuhan. Culture is our Business. 1970. McGraw-Hill.

15 Gerasimov. "The Value of Science", 2016.

16 Peter Pomerantsev. "How Putin is Reinventing Warfare", Foreign Policy. May 5, 2014. http://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/

17 NATO Cooperative Cyber Defence Centre of Excellence. "Tallinn Manual 2.0." 2017. https://ccdcoe.org/tallinn-manual.html

18 Bruce McClintock. "Respond to Russia's Information Warfare." U.S. News and World Report. https://www.usnews.com/opinion/world-report/articles/2017-07-17/the-us-needs-a-response-to-russias-information-warfare