Testimony submitted to the

Commission on Security and Cooperation in Europe
U.S. Helsinki Commission

September 14, 2017

The Scourge of Russian Propaganda: Evaluating Russian Information Warfare and Shaping the American Response

Molly K McKew
CEO, Fianna Strategies

I am grateful for the opportunity to share some of my experiences countering Russian information warfare. I've spent the past decade watching the deployment of Russian information operations across the European frontier, including in Georgia, Moldova, Ukraine, and the Baltic states. I have done this primarily as a partisan, working for political actors and other groups being attacked by these Russian initiatives, so I tend to come at this from a different perspective than others. Russia is constantly acting, assessing, and refining their information capabilities, which have become an embedded and normalized part of our information landscape. We must be clear about what these measures aim to achieve and their impact, and bring a renewed sense of urgency to defending our nation.

* * * * *

Overview of Russia's information war against Western societies

It is essential that we evaluate the challenge of 'Russian propaganda' from the right perspective in order to develop effective counter measures.

First, disinformation is a means of warfare. It is the core component of a war being waged by the Russian state against the West, and against the United States in particular.

Second, the primary line of effort in this war is conducted in English. We have failed to secure our information space, allowing our self-defined 'primary adversary' to shape and in some cases control it at will, often blind to what they aim to achieve. This provides the Kremlin a significant strategic advantage.

Third, we have only just begun to understand the scope and scale of resources, formal and informal, that Russia devotes to information warfare — which means we have failed to understand the importance the Kremlin ascribes to these efforts. Some resources are devoted to forms we know — RT, Sputnik, etc — and others to forms we are coming to know — automated actors like botnets, and amplifiers like trolls — but far more of these measures are still deep within the shadow space, acting along parallel lines of effort.

It bears repeating: it's not propaganda; it's information warfare. It is, in many respects, the war that matters most. In our strategic thinking, information operations of this kind are meant to amplify military operations. In Russian doctrine, it is the other way around: military operations amplify information operations. The 'smoke and mirrors' are a primary means of power projection.

The information warfare being used against us aims to erode political will, in ourselves and our allies, to defend what defines us; to sow doubt and division, discord and chaos, in order to

reshape an environment where American power is less effective; to target the minds of our soldiers and leaders, activists and influencers, voters and citizens, using subversive means; to spark political unrest, and make us question that democracy can provide just, free, equitable, secure, and prosperous societies.

And it is working.

We have seen this type of information warfare deployed against other nations. There is ample evidence of the extent to which Russia will go to shape demographics, politics, and social structures in its near abroad, using military, economic, political, and cultural coercion. But we, as Americans, want to believe it doesn't work on us — that oceans are still a barrier to foreign invasion, that we are immune to these manipulations, particularly from an opponent far weaker, militarily and economically.

In their weakness, the Kremlin bets big. So far, the gamble has paid off — because for years they have been strolling across an open battlefield.

To secure our information space, we need an integrated understanding of the threat, and an integrated set of measures that can be taken to counter it, including:

- ***Enhanced clarity of the threat and its impact:*** We must clearly identify the tools and tactics being used against us in the information space, and effective means of disrupting them.
- ***Whole-of-government response:*** We need unity of mission to secure the American information space, including organizing our diplomatic, military, and intelligence assets to counter information warfare via a whole-of-government approach. Nongovernmental assets and actors also play a vital part in any effective response, and should be creatively engaged.
- ***Rethinking authorities:*** We must reevaluate the role of US military/counterintelligence actors in securing our information space during this time of rapidly escalating threats. Our most experienced assets should not be boxed-out of defending the American people.
- ***Develop rapid response capability for irregular information warfare:*** Build capacity to execute local rapid information operations (positive and interceptive) manned by sanctioned irregulars (US Special Forces and counterintelligence assets, plus independent actors).
- ***Give Americans defensive tools:*** This occurs via three strands. First, speaking clearly to the public about the threat. Second, developing practices for enhancing national 'cognitive resistance,' particularly in groups being targeted by Russian operations. Third, building stronger data/privacy protections for Americans to limit the coercive applications of 'big data.'
- ***Motivate/activate the American populace:*** We need political leaders with the will to speak clearly to our people about our principles and values — the narratives and truths that matter.
- ***Whole-of-alliance approach to securing the information space:*** A better-coordinated US response mechanism will be better positioned to collaborate with and lead our NATO/EU allies in countering Russian information operations. A range of different mechanisms have been developed by certain European military, government, and civil society actors that would be greatly enhanced by clear strategic goals and supporting resources.
- **Social media evaluation/regulation:** Adversarial forces are using social media platforms to attack our societies. We need to consider applying rules to how paid and automated content can be spread through social media. This is not about limiting the free flow of information and ideas — we should never seek to emulate Russian control tactics or the means used by other authoritarian states — but restricting the ability for coercive targeting and the simulation of human supporters/movements to promote coercive propaganda.
- **Enhanced understanding of aims of Russian financial flows:** Russian disinformation has purpose. So does the export of its capital. We must be far more aware of the aims of this financial flow, especially investments into/partnerships with American technology companies.

These measures will be discussed further in the final section.

There is an urgent need for effective counter measures. Russian efforts fuel conflict and chaos in Europe, the Middle East, Afghanistan, Asia, and the Arctic. While our attention is elsewhere, spread thin across crises and putting out fires, the other tools in Russia's guerrilla arsenal have time to gain vantage. This arsenal is backed by considerable state financial resources. We have a tendency to see Russian kleptocracy as a means of buying super-yachts and penthouses. It isn't. It's about buying us. The range of tools this money supports is unnerving in its informality, depth, and potential.

Russia's war in Syria has been a giant arms expo meant to demo and sell a new generation of Russian weaponry. The Russian information control model is just as much on display and in demand. President Putin recently discussed the opportunities and perils of artificial intelligence, adding: "We will certainly share our technology with the rest of the world, the way we are doing now with atomic and nuclear technology."[1] We have every interest in preventing the proliferation of effective tools and models of computational propaganda[2].

Ten years since a cyber attack on Estonia, nine years after Russia's invasion of Georgia, almost four years since the invasion of Ukraine, ten months since we got a red alert on the information war being waged against the American people — and our actions says we're still trying to decide if this is a threat that we need to take seriously. For example: Congress mandated the creation of the State Department's Global Engagement Center to help counter Russian disinformation, authorizing considerable financial resources to the cause. These resources have neither been allocated nor spent[3]. Other efforts have directed resources to countering Russian narrative — in Russian[4]. Very little has been done about the English language disinformation targeting Americans.

Russia has corrupted our information space through countless means. Right now, there are efforts to analyze the war; expose the war; map the war — but very little is being done to *fight* the war, or to provide resources, mandate, or authorities to those with the skill sets to do so. While we investigate and analyze and discuss, the diverse initiatives underway from the Kremlin have accelerated in Europe, across the globe, and in the United States.

* * * * *

Understanding the aims of Russian information warfare: Examples from the field

Information tools are the new superweapons — like chemical weapons in WWI or the atomic bomb in WWII, they shift the fundamental balance of power and fear. In their essence, Russian measures aim for the complete domination of an information landscape in order to influence the minds of a population. These measures target, in particular, military personnel, political leaders, and vulnerable, disenfranchised, and unmoored elements of society — but they also target society writ large by focusing on identity, historical memory, topics of a divisive nature, and more. These measures aim to harden specific aspects of identity; to radicalize elements of society; and to build the activation potential of a population.

Disinformation can be lies or partial truth. What matters is that it has purpose. It is targeted against specific parts of a population using crafted narrative, and it aims to mobilize groups of people to act in specific ways. So this is not about words, but about achieving concrete results. Ideas lead to decisions; once a decision is made, it will be rationalized, entrenching the idea.

The technological tools of producing, disseminating, and amplifying disinformation matter — but far less than the construction of that information to be persuasive and coercive against the audience. In this regard, two things matter: narrative and storytelling. *Narrative* is the overarching construct of the information, providing answers to questions of who we are and why things are the way they are. *Storytelling* is how you build and transmit narrative.

"What did it aim to achieve?" is a more important question in evaluating disinformation than what is true. Fighting it must also have a purpose. If we aren't clear what that purpose is — what we are fighting for, what we believe — then we can't win.

Russia goes to great pains to downplay their role in information operations because exposing them can restrict their freedom of movement. Some of the most effective Russian disinformation aims to make you believe Russia is weak and disorganized, and the Kremlin excels at finding local actors to act as masks and passthroughs. There can be many different lines of effort aiming to achieve different outcomes in different audiences. But there is a pattern and a texture to how these efforts form and coalesce, to the narrative they use, and to the results they can yield. Below are a few examples from my own experiences.

***Shaping the Baltic information environment*:** During the past year, I worked as the strategic director of a project to enhance Baltic Russian-language media. This was a modest initiative, primarily small grants to journalists and producers. Nonetheless, I can document about six attempts by Kremlin-connected actors to gain access to the project and our work. This illustrates how deeply dominance in the Baltic information environment is a preeminent concern of Russian efforts.

In the Baltic states, there is a basic three-pronged approach: rewriting history, demonizing NATO, and sewing doubt about the efficacy of pro-Western governing forces. Understanding the narrative of these operations is critical: efforts to demonize occupation-era Baltic resistance movements or deny the existence of a pact between Stalin and Hitler sometimes seem obscure to us, for example, but the purpose is to create justification for modern Russian state actions and ambitions. These nations are inundated with Russian and English language content generated by the Russians as they aim to shape the perception of specific groups. Russia also shapes the external narrative on the Baltics by providing English language news from the region. A recent report found that computational propaganda plays a significant role here: a quarter of the accounts posting in English on Twitter in the Baltics and Poland were likely bots/automated, responsible for 46% of the total English language content on NATO[5].

Moldovan identity politics: Unlike the Baltic states, Moldova does not have a strong national identity and is quite divided as a society. It also has a terrible information environment, with most of the national media controlled by the nominally pro-Western oligarch whose party has captured most of the governmental institutions. This is fertile ground for propaganda and information operations, particularly nasty personal attacks — but the way information moves and is used helps to expose agendas, in many respects. In the last presidential election, for example, which was won by the pro-Russian candidate, the media holdings of the 'pro-Western' oligarch mentioned above amplified Russian attacks and disinformation against the pro-European candidate in the race[6].

In Moldova, false information is also frequently introduced via Russian information channels to create positive sentiments about the unpopular ruling force — a phenomenon we called 'double disinfo,' disinformation meant to make another piece of untrue information believable. A recent example of this had pro-Russian social media accounts leak a fake letter in which USAID complained to the ruling party that they were not doing enough to fight Russian information in Moldova[7]. When the letter was exposed as a fake, the false counter-positive — that the ruling party was fighting Russian information — is made more believable.

Voter mobilization/suppression in Georgia: Georgia's parliamentary elections in 2012, during which I worked as an advisor to the Georgian National Security Council, were the first where I saw Russian-connected political forces looking to hire Western firms who could teach them about micro-targeting and other social media-based information tools. American teams marketing themselves as contributors to the Obama victory were hired by Bidzina Ivanishvili to operationalize black information campaigns, which contributed to getting tens of thousands of people in the streets before the election. Most of what was happening in the social media

landscape was completely opaque to the ruling party until well after the election: the messaging was designed not to touch anyone who was a consistent supporter of the government.

One aspect of this overall campaign that I would highlight as a favored Russian tactic: the use of diversion. The online media campaigns cultivated an intense environment of fear of the potential for violence — rumors that the government would declare martial law instead of holding the vote; claims Russia would invade again if the ruling party won; threats of disruption and violence at the polls. This consumed the attention of the government/ruling party and the diplomatic/observer community. But this was always meant to be a distraction from real lines of effort: black media campaigns and traditional voter mobilization efforts. I mention this because I believe there was a similar Russian diversion effort during the US elections: US intelligence and the Obama White House feared disruption of our elections via the hacking of electoral and voting infrastructure, and significantly less attention was paid to the information operations being run. In both cases, the lesson we should learn: information operations are a primary line of effort from the Kremlin.

Narrative themes during elections/referenda: While every now and then there is a Marine Le Pen — an openly pro-Kremlin political candidate — arguably the more dangerous new archetype of candidates favored by the Kremlin are those who amplify Kremlin narrative as part of their political platforms without being so openly pro-Russian. These themes can include: nationalism/anti-globalism/anti-integration; anti-refugee/anti-immigration; 'traditional' identity and values; anti-tolerance, especially anti-LGBT sentiments; to name a few. Knowingly or not, parties focusing on these themes contribute to achieving core goals important to the Kremlin — rejecting Western liberal democracy; weakening NATO, the EU, and the transatlantic alliance; deepening divides inside our alliances and our nations that can be exploited. This model is critical in many countries, especially some former captive Soviet nations, where pro-Russian political forces would be unable to gain significant following. But the governing agendas of these parties tend to be more inward looking and de facto downplay the significance of the existential threat from Russia, on which the basic line tends to be: "Wouldn't it be nice if we had a better relationship with Russia (especially economically)?"

The degree to which Russia exploits this ideological space, sometimes very tactically, should not be underrated. Some groups knowingly engage the Kremlin for resources and support, glad to have an ally; others may receive support via amplification in Russian information architecture, whether they asked for it or not. Anti-LGBT sentiment has been a vital avenue for the Kremlin to cultivate a new generation of political and cultural allies across Europe and the United States. In elections across Europe in the past two years, anti-refugee and anti-migrant sentiment has been used repeatedly to galvanize nationalistic voters; this has been a core theme deployed in the German elections which will be held later this month, as it was used before in France and the Netherlands and the Brexit referendum. Just this week, we have news that Russian accounts on Facebook were used to organize anti-immigrant rallies in the US during our election[8]. There are dozens of examples that could be given, but that one makes it the most clear: this isn't just information but the hope to elicit behavioral change.

* * * * *

Assessing the state of conflict and readiness in the information war

In order to propose defensive and offensive information warfare strategies, it helps to define the current doctrinal and strategic landscape clearly. This starts with the 'Gerasimov Doctrine.' The Gerasimov Doctrine builds a framework for the use of non-military tactics, including information warfare, that are not auxiliary to the use of force but the preferred way to conduct war. Chaos is the strategy the Kremlin pursues, aiming to achieve an environment of permanent unrest and conflict within enemy states and alliances where a weak Russian state can exert outsize influence and control[9]. But we've been talking about the Gerasimov Doctrine like it's the holy grail of understanding Russia since 2013. We reanalyze it over and over. Meanwhile Russian

doctrine has evolved further, articulating how to apply these core concepts across multiple strands of warfare.

The Value of Science is in the Foresight Gen. Valery Gerasimov, Russian Chief of the General Staff **Feb 2013**	*In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace… The very "rules of war" have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness… All this is supplemented by military means of a concealed character…**The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy**… Among such actions are the use of special-operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected.*
The World on the Verge of War Gerasimov **March 2017**	***The military strategies applied by the leading nations stipulate that dominance in information space is essential in warfare.** This task requires engagement of media and social networks. They are complemented by information, psychological, and technical influence…. The [Russian] Armed Forces are currently gaining their combat experience in Syria. They have a unique opportunity to test modern weapons and military equipment in adverse climate conditions. It is necessary to continue this military practice in the Syrian campaign and draw the lessons to adapt and improve Russian weapons… It should be noted that victory depends not only on the material but also the spiritual resources – the nation's cohesion and desire to confront the aggressor at all cost.*
The Guerrilla Payees Konstantin Sivkov, retired General Staff officer **April 2017**	*The evidence points to new types of military action in upcoming conflicts. Our 20 years of experience insist on the importance of irregular forces (guerrillas). They are integrated into military personnel and excel at combat endurance. **Furthermore, irregular operations achieve the most political goals of war.** If guerrilla forces fail, defeat is imminent, regardless of conventional and special forces superiority… Guerrillas are capable of large-scale operations and consistent military action pursuing tactical and strategic goals… Coordination with guerrillas is always complicated. Nonetheless, their actions must be coordinated with the regular armed forces, in particular during special operations. In other words, WWIII guerrillas must be under the authority of a single commander. Thus, these unique forces are vital for the Russian Armed Forces…. If provided with the information and intelligence available to the regular armed forces, even small numbers of irregular troops can produce immediate results.*

What we see in these excerpts[10]: Russia is operationalizing a fundamentally guerrilla approach to total warfare in order to achieve strategic political objectives — a global imperialist insurgency.

Both the United States and Russia, for different reasons, have made the determination that fighting and defending against unconventional warfare is the key to future war. But we pursue it differently. The US has shifted toward special operators and the use of drones; training partner nations, and helping them conduct strikes on targets; running defensive information operations; bolstering our efforts with civilian-military affairs projects. Russia does everything else. The nature of their efforts is not defensive or retaliatory, but entirely offensive.

The Kremlin is recruiting people, groups, and societies into a dirty war.

* * * * *

Securing our information space is about English language information, not Russian

When we speak of 'Russian propaganda,' we don't really mean Russian *language* propaganda as much as we mean Russian state efforts to export disinformation into local languages in many European countries, and into English in particular, which have drastically accelerated since 2013. Russia invests heavily in media resources; learning, creating, and adapting tools for targeting information to specific individuals; and automating disinformation across social media platforms in ways to reach specific people, counter/promote specific ideas, and game algorithms to give primacy to the Russian version of 'truth.' In many respects, our entire information space has been corrupted by or made vulnerable to Russian information operations.

The Russian language space, in comparison, is controlled, insular and collapsing on itself without captive nations — as the chairman of the Duma Committee on Education and Science recently noted, while railing against the 'linguistic hegemony of English,' the number of Russian speakers has declined by 50 million people since 1991[11].

But the 'linguistic hegemony of English' also makes us vulnerable. Disinformation is more powerful in English because English is the language of the internet. It's a bigger echo chamber, and it gives more reach to target audiences vulnerable to core parts of Russian narrative. The US also has incredibly weak data/privacy protections, thus enabling the harvesting and analysis of data for cognitive targeting in ways that should make us profoundly uncomfortable.

Looking at information warfare as a map exercise: Russia has used disinformation to project the line of conflict forward, further from their borders — to effectively erase borders while creating the virtual 'buffer zone' they can't have territorially. Our immediate response should seek to mirror this — not by addressing a problem hundreds of miles behind the line of conflict (Russian language) but by moving the line of conflict further from our country, back toward the aggressor. If this war has no borders, it is a fluid space that we must constantly expand and enhance not to lose. In real terms, there is no 'defending' the information space. The only defense is offense — illuminating and educating people on the threat, and promoting our principles and values.

Russia likes to position all their doctrine as a 'response' to Western actions. A more helpful way to gain insight into what the Kremlin believes they can achieve with unconventional warfare, and with information warfare in particular, is to understand that all the tools they deploy against us, they used against the Russian people first. We need to secure our information space, just as we would any other border. The Russians did this to their own information space before invading ours — building parallel social media, controlling access to content, flooding the local media landscape with free entertainment content, shutting down most of the independent media, now using automated social media content to amplify and bury specific views.

* * * * *

An integrated strategy for securing our information space

There are four key groups for crafting an effective response to Russian information operations: *government* (including military, intelligence, etc); *industry* (tech and data companies); *civil society*; and *citizenry*. Government plays an essential coordination role.

These are complicated issues, touching on freedom of speech and expression, national security, and more. We cannot use the same means of information control as the Kremlin to secure our information space. Our mirror-world version of Russian information control: not to control the internal information environment, but ensure its integrity; not to harden views, but to develop positive cognitive resistance efforts to build resilience in our population; not to argue that there 'is no truth,' but to promote the values and idea that we know matter.

Securing our information space has less to do with cybersecurity than building resilience in our citizenry, and re-crafting the ways that information can be introduced into and spread across our networks. I will expand on the measures proposed in the first section below, touching briefly on the non-governmental actors before focusing on what our government can do.

CIVIL SOCIETY — including journalists/investigative journalists and initiatives to track and document Russian influence operations — plays a vital role in both bringing ***enhanced clarity about the threat*** and ***giving Americans defensive tools*** via enhanced awareness of Russian information operations and what they aim to achieve; exposing Russian information campaigns and the networks that amplify them; and tracking and illustrating how Russian influence operations work, more broadly. In the future they will also play a vital role in restoring our collective resistance to hostile influence operations. This requires creativity, and resources being directed to civil society initiatives should tolerate some degree of experimentation and failure.

CITIZENS need to be more aware of their information environment. I believe this is a more complicated effort than the promotion of media literacy and fact-checking alone.

INDUSTRY, in particular social media and tech companies, bear a special responsibility in our efforts to respond to Russian information warfare — to remove or contain Russian information architecture from our system. But there are broader questions. After the 2016 election, there was a lot of discussion about Americans 'choosing' to inhabit separate information universes. But what isn't discussed: this is not always a choice, but something being done to us — by targeted advertising, by promoted content, and by algorithms that tell us what we want to see — algorithms that Russian data scientists and information warriors aptly know how to game.

Micro-targeting, hyper-targeting, and individual targeting on social media have one primary application, in a variety of forms: radicalization.There are some uncomfortable questions to be asked here, about whether social media platforms are blindly or knowingly enabling the means for mass psychological operations to radicalize societies and deepen divisions, and whether there are accountability measures required. Facebook in particular has created a means of mass surveillance and collection, and a means of operationalizing information operations effectively and inexpensively — which it acknowledges but downplays[12]. Despite detailed explanations why they bear no legal or moral responsibility for what their engineering has created, Facebook is essentially a real-life, free-market 'big brother' — a platform for surveillance and computational propaganda available to any power willing to pay for it.

The same Russian intelligence-connected company that previously staged a test information assault against the United States — an attack meant to instill fear and mobilize panic[13] — was allowed to buy political advertising targeting Americans during elections[14]. As long as social media platforms refuse to acknowledge the tools and tactics they are enabling, promoting, and profiting from — and explain why they will not take more aggressive steps to protect data privacy, remove revenue possibilities from propagandists, and ensure that content automation isn't gaming algorithms to subvert the minds of human users — then we need to be more aggressive in educating our population about how they are being attacked in the information space and exactly what these attacks aim to achieve. So far, Americans have been offered little clarity of leadership in this regard.

GOVERNMENT plays a vital role in coordinating an effective response to Russian information warfare. This is particularly true in two areas: *political will* and *structural response*. Both are critical, but the importance of political will cannot be undervalued. For example, in Europe, there have been new institutional actors introduced — including the NATO and EU Centres of Excellence, and the EU's East Stratcom Task Force — as well as support given to a range of civil society initiatives — including think tanks like European Values[15] — but the lack of central political will to mount an effective strategy against Russia undercuts these smart initiatives. Our alliance would benefit from American political will galvanizing a ***whole-of-alliance approach to securing the information space***.

In the US, I hope political will be in abundance when ***enhanced clarity of the threat and its impact*** are provided. To counter what is being done to our society by a foreign adversary, we need a ***whole-of-government response***. The Russian operational footprint in Europe relies on a core of SVR/FSB/GRU resources, with access to significant technology and information capabilities, operating in a broad lane that asks for creativity and doesn't punish failure, backed by state resources. We have the architecture to be able to build a more effective task force — but we don't. Unity of mission is critical. We need a 'star chamber' coordinating our best assets — diplomatic, military, intelligence, industry, nongovernmental, and informal — to counter the information warfare launched by the Kremlin's 'power vertical.'

Irregular warfare — including information warfare — will need to be fought within our borders. We should define how we do that before the next crisis. To bridge our capabilities gap on an accelerated timeline, we need to review our resources for countering threats in the information space, and we need to ***rethink authorities***.

We have forces designed for unconventional warfare: US Army Special Forces. In Europe, for countering Russia, that's the 10th Special Forces Group. This is a group of regionally-aligned, culturally-astute, deep-knowledge forces with the expertise and capabilities to work with local partners to amplify efforts and address critical needs. But practically speaking, they lack the resources, mandate, and technology to act. Instead of giving 10th SFG added resources to ***develop a rapid response capability for irregular information warfare,*** conduct Military Information Support Operations (MISO), operate in a wider lane in non-conflict countries alongside the State Department in countering these aggressive threats, and coordinate other military and defense assets in this area — this expertise is still in a box. The Marines have recently established a 4-star office dedicated to information operations, led by the Deputy Commandant of Information. There is a whole branch of the Pentagon that specializes in this area. We need this expertise engaged in the fight, and we need to remember that our mil-mil relationships are the steel in the architecture of NATO, which is reinforced by the intelligence backbone of the 'Five Eyes' community.

There is a similar challenge with authorities for US counterintelligence, especially for the FBI and especially in the information space[16]. The Russians have identified a giant blind spot where they can operationalize influence with no interference or oversight (social media). We have to change that equation without falling into the trap of replicating Kremlin tactics.

Clarity on the threat is one of the primary means of ***giving Americans defensive tools*** against information operations, and engaging them these issues will help ***motivate the American populace*** and enhance resistance. It is vital to evaluate whether ***regulatory measures*** can be legislated to enhance data/privacy protections for Americans, limit coercive applications of data-driven targeting, and bring transparency to paid content on social media platforms. Again, this is not about limiting the free flow of information and ideas, but restricting the ability for coercive targeting and the simulation of human supporters/movements to promote coercive propaganda.

Finally, government can apply its capabilities in tracking hostile foreign financial flows to ***enhance understanding of how Russian money moves in our system***, and what it aims to achieve. President Putin is not some all powerful being. But he has certainty and seeks to build a cynical world were the only thing that matters is money. That is the 'ideology' the Kremlin exports. And until we understand how that money is poisoning our system of beliefs, he wins.

* * * * *

Our primary failures when it comes to responding to information warfare are failures of imagination, clarity, and coordination. We don't wargame the shadow war. We need to. This is a war we must win.

[1] Putin's remarks can be read here in English: https://sputniknews.com/russia/201709011057000758-putin-school-children-world-lord/

[2] *Computational propaganda is the use of automation — including tools like botnets and artificial intelligence (AI), directed by algorithms and the harvesting of data to create targeting profiles — to influence opinion via the internet and social media*

[3] Toosi, Nahal. "Tillerson spurns $80 million to counter ISIS, Russian propaganda." *Politico.* Aug 2, 2017. http://www.politico.com/story/2017/08/02/tillerson-isis-russia-propaganda-241218
Toosi, Nahal. "Tillerson moves toward accepting funding for fighting Russian propaganda." *Politico.* Aug 31, 2017. http://www.politico.com/story/2017/08/31/rex-tillerson-funding-russian-propaganda-242224

[4] CBS News. "U.S. launches TV network as alternative to Russian propaganda". Feb 9, 2017. https://www.cbsnews.com/news/us-current-time-tv-network-rfe-russia-russian-propaganda-misinformation-rt/

[5] NATO Stratcom COE. *Robotrolling* 2017/1. http://stratcomcoe.org/robotrolling-20171

[6] Jamestown Foundation. "Moldova's De Facto Ruler Enthrones Pro-Russia President." *Eurasia Daily Monitor Volume: 13 Issue: 196.* December 14 2016. https://www.ecoi.net/local_link/333654/461950_en.html
Vlas, Cristian. "Old Fashioned Skulduggery Overshadows Elections in Moldova." Emerging Europe. Nov 19, 2016. http://emerging-europe.com/voices/voices-intl-relations/old-fashioned-skulduggery-overshadows-the-elections-in-moldova/

[7] The source of the letter was: https://twitter.com/Urugvayintellig/status/904633014541574144/photo/1

[8] Collins, Ben, Kevin Poulsen, Spencer Ackerman. "Russia Used Facebook Events to Organize Anti-Immigrant Rallies on U.S. Soil." *The Daily Beast*. Sept 11, 2017. http://www.thedailybeast.com/exclusive-russia-used-facebook-events-to-organize-anti-immigrant-rallies-on-us-soil

[9] McKew, Molly. "The Gerasimov Doctrine." *Politico Magazine.* Sept/Oct 2017 ed. http://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538
McKew, Molly. "Putin's Real Long Game." *Politico Magazine.* Jan 1, 2017. http://www.politico.com/magazine/story/2017/01/putins-real-long-game-214589

[10] *The Value of Science is in the Foresight* — https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/*; The World on the Verge of War* — http://vpk-news.ru/articles/35591*; The Guerrilla Payees* — http://vpk-news.ru/articles/36159

[11] The remarks can be read here in English: https://themoscowtimes.com/news/russian-language-losing-out-of-english-hegemony-says-official-58779

[12] Shane, Scott. "The Fake Americans Russia Created to Influence the Election." *New York Times.* Sept 7, 2017. https://www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html
http://www.politico.com/magazine/story/2017/09/08/how-facebook-changed-the-spy-game-215587

[13] Smith, Rohan. "Columbia Chemical hoax tracked to 'troll farm' dubbed the Internet Research Agency." news.com.au. June 4, 2015. http://www.news.com.au/technology/online/social/columbia-chemical-hoax-tracked-to-troll-farm-dubbed-the-internet-research-agency/news-story/128af54a82b83888158f7430136bcdd1

[14] Shane, Scott & Vindu Goel. "Fake Russian Facebook Accounts Bought $100,000 of Political Ads." *New York Times.* September 6, 2017. https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html

[15] For European Values' recommendations on how responding to hostile disinformation operations, see: http://www.europeanvalues.net/wp-content/uploads/2016/06/Full-Scale-Democratic-Response-to-Hostile-Disinformation-Operations-1.pdf

[16] Rangappa, Asha. "How Facebook Changed the Spy Game." *Politico Magazine.* Sept 8, 2017. http://www.politico.com/magazine/story/2017/09/08/how-facebook-changed-the-spy-game-215587