



02

# THE NEXT CENTURY OF PSYOP

---

## Psychological Operations and the 21st Century Operating Environment.<sup>01</sup>

BY ADAM L. SILVERMAN, PhD

---

As Psychological Operations enters its second century, the global system, international relations, foreign affairs, the global operating environment and the U.S. standing in the world are vastly different than they were in 1918. In the post 9/11 era, the U.S. remains the sole superpower in a global system that is in many ways a legacy of the Cold War world. Its two closest great power challengers are an aspirant to that status in China, and the claimant to the Soviet Union's legacy in Russia. Neither China nor Russia currently have the capabilities to militarily challenge the U.S. for hegemony. And there are a number of non-state actor threats that, while they certainly present a nuisance to the U.S., its allies and its partners, do not actually present an existential threat. ISIS or al-Qaeda do not now, and never had, the capabilities to bring down the U.S.

There is, however, one constant between 1918 and today. As World War I was ending, or perhaps, more accurately transforming into a series of low intensity conflicts that would simmer until reigniting into World War II,<sup>02</sup> the great power competition was changing. Specifically it was adding a major new complication: a clash of ideas. These ideas were about how to better

organize state and society. And they placed the ideas of liberty and liberal democracy in all of its various types in direct conflict with the totalitarian ideas of fascism on the extreme right and communism on the extreme left. Just as different forms of liberal democracy would develop, so to would different variations of fascism and communism. These clashes of ideas, of how states, societies, and even the global system should best be structured, would lead to both World War II, a long Cold War, the Korean and Vietnam Wars, and a number of conflicts fought by the proxies of the two post World War II superpowers. That Psychological Operations as a military occupational specialty would grow up and mature in this war of ideas is not surprising. As fighting bad ideas with better ones is part of the core mission of Psychological Operations.

02

**Given that so many of the dangers and threats that we face in the 21st Century Operating Environment are asymmetric, irregular and unconventional attempts to leverage terrorism and offensive cyber operations to convey information for effect, the 21st Century should be the new Psychological Operations' century.**

U.S. ARMY PHOTO BY STAFF SGT. CHAD MENEGAY

As Psychological Operations enters its second century, the world is once again faced with a war of ideas. The ideas of liberty and its expression in the different types of liberal democracy are once again facing off against totalitarian ideas from both state and non-state actors. Vladimir Putin challenges the U.S. and its European Union and NATO allies and partners with his promotion of managed democracy as a façade for the kleptocratic organized crime state he has created in Russia.<sup>03</sup> Xi Jinping, recently declared as President for Life, promotes his fusion of Maoism, state-controlled capitalism, and Chinese nationalism through his One Belt and One Road Initiative.<sup>04</sup> ISIS continues to promote an extreme version of *tawheed*, the Islamic theological understanding of the unity of the Deity, which includes violently imposing its doctrine on believers and unbelievers alike.<sup>05</sup> There is one major difference, however, between the 20th Century



01

war of ideas that stretched from World War II through the post-Cold War period. In the 21st Century Operating Environment, the theater of operations is as likely, if not more likely, to be the cyber domain than the Land, Sea, or Air domains. The Cyber Somain, which is everywhere and nowhere, exists within and without the continental United States at the same time, is perfectly suited for Psychological Operations. As a result, the 21st Century Operating Environment should be the new Psychological Operations century.

## THE 21ST CENTURY OPERATING ENVIRONMENT

*The National Security Strategy*<sup>06</sup> released in December 2017, focused on a return to great power competition as the core of instability in the global system and the 21st Century Operating Environment. Without always being explicit, it conceptualizes a great deal of



02

the relations in the global system as being part of the interactions between the U.S. as the legacy superpower from the Cold War, China as a rising and emerging power, and the attempts of Russia to function as the great power legacy of the Soviet Union despite not actually having the capacity to do so aside from its nuclear arsenal. *The National Security Strategy*, by using this characterization of the 21st Century Operating Environment as both a return to an earlier period of great power competition melded to 21st Century concerns, such as the abuse, manipulation and weaponization of the Cyber Domain, provides us with a good starting point for considering where Psychological Operations should go in its second century.

The great power competition that *The National Security Strategy* delineates is not simply a recreation of the late 19th and early 20th centuries' great game. Rather it recognizes that America's competitors are approaching this competition, and will continue to do so, through asymmetric, irregular and unconventional means; though not always in the way that we doctrinally define these terms. In many ways, just as the core of the 20th Century's dispute was a battle of ideas — between liberty and totalitarianism on both the right (Fascism) and left (Communism) extremes, between democracy in its different variations, Fascism, and Communism — so too, is the 21st Century Operating Environment a war of ideas. A war of ideas between the real liberal democracies, whether a Republic like the U.S. and France or parliamentary democracies like



the United Kingdom and many of the EU and NATO member states, Putin's idea of managed democracy — a democratic facade running in front of a kleptocratic organized crime state, China's blend of Maoist Communism and state controlled capitalism, or ISIS's extremist understanding of *tawheed* — the radical unity of the Deity. The major difference, however, is our technological advances have moved ever more of these battles from the physical battlefield into the Cyber Domain. The campaigns in the 21st Century war of ideas will not be fought at the Somme, Belleau Wood, Normandy, Remagen, Pelilue, Guadalcanal, Cho Sin, Khe Sanh, Tora Bora or Ramadi. Rather, more and more of them will be fought on Facebook and Twitter, 4Chan and Reddit. And unlike people, ideas are almost impossible to kill; especially so with weapons. Bad ideas can only be killed with better ones. As Bernard Fall stated in *The Theory and Practice of Insurgency and Counterinsurgency* (emphasis mine):

***One can't fight an ideology; one can't fight a militant doctrine with better privies. Yet this is done constantly. One side says, "land reform," and the other side says, "better culverts." One side says, "We are going to kill all those nasty village chiefs and landlords." The other side says, "Yes, but look, we want to give you prize pigs to improve your strain." These arguments just do not match. Simple but adequate appeals will have to be found sooner or later.***<sup>07</sup>

Because of the improvements of technology and their effects on great power competition, as well

## THIS NEW FORM OF GREAT POWER COMPETITION FOR THE 21ST CENTURY IS PRIMARILY UNCONVENTIONAL ... IT LEVERAGES OTHER FORMS OF NATIONAL POWER TO ACHIEVE ITS STRATEGIC OBJECTIVES. IT IS ALSO PRIMARILY NON-LETHAL.

as their own internal limitations, America's great power competitors are both unable and/or unwilling to challenge the U.S. using lethal means. They are also unable and/or unwilling to challenge using conventional means. China is not yet prepared, despite naval challenges in the South China Sea, to actually challenge the U.S. for the role of military hegemon in the Asian-Pacific area of operations. The People's Liberation Army's Navy is still not ready for that confrontation. Nor is China ready for, let alone trusted by its neighbors to, secure the sea lines of communication and commerce. This has resulted in China continuing its long-term strategy of heavily investing in building up the PLAN while also funding the U.S., through the purchase of about 8 to 11 percent of our foreign-held debt, so that the U.S. will have the funding to continue in this role until China is ready to challenge it for that role. The One Belt and One Road initiative is also part of this strategy. One of the objectives of the initiative is an attempt to generate good will within China's neighbors and partners, through investment and development,<sup>08</sup> which will be needed in order for China to one day challenge the U.S. The attempt by China to change the attitudes and feelings towards it through the Belt and Road initiative is a good example of the Psychological Operations' effects they have built.

Russia, as the other great power challenger, is simply unable to challenge the U.S. directly. Russia isn't even in the top 10 largest economies in the world.<sup>09</sup> Even if we don't count individual U.S. states as independent economies. Both California and Texas have larger economies than Russia's, and unlike Russia's, theirs' are more diversified and growing. Russia's military, despite Putin's buildup over the past several years,<sup>10</sup> is still a pale shadow of the Soviet military. Russia's one aircraft carrier, after a month's long deployment in support of Russian interests and operations in Syria, is now in dry dock for refit,<sup>11</sup> where it will remain until 2024. While China is not yet ready to challenge the U.S. military, Russia is not able to. This has led to the development of a different strategy: the weaponization of the Cyber Domain for psychological, information and cyber warfare, as well as a return to classic Soviet-style network.

01. 02

Road development in Nepal is a major concern for the underdeveloped nation as it seeks to meet the need for connectivity, creating employment and increasing trade.

A 2017 memorandum of understanding between Nepal and China helped fill the financial and material void the nation faced in bridging the infrastructure gap and will ultimately connect Nepal to China, Central Asia and Eastern Europe as part of China's One Belt and One Road Initiative. The U.S. National Security Strategy recognizes that America's competitors, such as China, are approaching the power competition through asymmetric, irregular and unconventional means. As a long-term strategy, China is using Psychological Operations by leveraging this initiative to generate good will with its neighbors and partners, through investment and development, achieving its strategic objectives through non-lethal means.

U.S. ARMY PHOTOS BY  
JENNIFER G. ANGELO

This new form of great power competition for the 21st Century is primarily unconventional, but not necessarily how we define unconventional warfare. It leverages other forms of national power to achieve its strategic objectives. It is also primarily non-lethal. Or it is non-lethal in how we usually and doctrinally define lethal action. For instance, it was reported that Russia's cyber operators hacked into, and interfered with, the operations of Saudi petroleum facilities in March 2018.<sup>12</sup> Russia didn't put steel on steel, but they achieved a physically lethal result — taking down Saudi petroleum operations — by leveraging expertise in the cyber domain. The Russian cyber attack on Saudi Arabia leveraged expertise in the Cyber Domain, just as it leveraged that same expertise in pursuit of its psychological operations against the U.S., the EU and NATO. These operations are estimated to have cost Russia approximately 1 percent of its military budget.<sup>13</sup>

The 21st Century Operating Environment is not simply one of great power competition. We still face ongoing threats from non-state actors. These threats are, as they have been since before 9/11, both asymmetric and irregular. As an example, the ISIS attack on the Paris suburb of St. Michael in late 2015 used the irregular, low-intensity warfare tactic of terrorism in pursuit of what is actually a psychological operations strategy.<sup>14</sup> St. Michael is known for being the suburb for immigrants in Paris. In the 1920s and 1930s it welcomed and integrated Italian, Spanish, and Portuguese immigrants into the political, social, and economic life of the community. It did the same thing for Algerian immigrants in the 1950s and 1960s. More recently it has done it for immigrants from the Middle East, Central and Southeast Asia — all predominantly Muslim. St. Michael was not picked by ISIS because it was a particularly soft target, or a softer target than others in/around Paris in 2015, it was picked in an attempt to achieve specific psychological operations effects as a result of the attack.<sup>15</sup>

ISIS's stated strategic goals include forcing Muslims to make a choice between ISIS's understanding of Islam, which requires all Muslims to either relocate to the caliphate or fight against non-Muslims and apostates where they reside outside the caliphate, and to force non-Muslim majorities to turn on their Muslim minorities. The intention of the attack was to turn the other residents of St. Michael, as well as the French, other Europeans and Americans against Muslims.

Specifically, so that there would be restrictions on taking in refugees from ISIS's war in the Levant and to crackdown on immigration from Muslim majority countries. The goal was to collapse one's citizenry or resident legal immigrant or refugee status into the binary of Muslim versus non-Muslim. ISIS targeted St. Michael in the attempt to demonstrate to the Muslims it seeks to influence that even a welcoming place like St. Michael was not Dar al Islam — the House of Peace, but actually Dar al Harb — the House of War. And, as a result, they had to either flee to the caliphate or fight. The targeting of St. Michael was also intended to convey to their non-Muslim fellow citizens that their Muslim neighbors cannot be trusted; that any one of them could be an ISIS sleeper agent. ISIS pursues this strategy for its terrorist operations in the U.S., EU and NATO member states because it doesn't have the ability to achieve its objectives directly. So it uses terrorism as a tactic in a psychological operations strategy that uses the information conveyed by the terrorist attacks in St. Michael, Florence, London, New York, etc., for effect against the French, the British, Americans and other EU and NATO partners and allies so they will provide ISIS with outcomes that it has no ability to achieve on its own.<sup>16</sup>

## PSYCHOLOGICAL OPERATIONS AND THE 21ST CENTURY OPERATING ENVIRONMENT

Given that so many of the dangers and threats that we and our allies and partners face in the 21st Century Operating Environment are asymmetric, irregular and unconventional attempts to leverage terrorism and offensive cyber operations to convey information for effect, the 21st Century should be the new Psychological Operations century. Whether it is aspiring or fading great powers, like China and Russia, or non-state actors like ISIS, al-Qaeda, Boko Haram, etc., using the non-military elements of national power, weaponizing the Cyber Domain or utilizing terrorism and other forms of low-intensity warfare to convey information for effect, part of the solution to these challenges is more Psychological Operations.

Psychological Operations professionals will need to be proficient in offense, defense and maintenance operations to provide the U.S. with a robust resource against these state and non-state threats in the 21st Century Operating Environment. The Psychological Operations community must continue to engage in

**AND THIS STRANGE NEW WAR WE FIND OURSELVES IN WILL NOT BE WON, BECAUSE IT CANNOT BE WON, SIMPLY THROUGH HACKING, PLANTING VIRUSES AND MALWARE, AND TIGHTENING DOWN CYBER SECURITY PROTOCOLS TO MAKE AMERICAN AND ALLIED SYSTEMS MORE SECURE AND RESILIENT. IT CAN ONLY BE WON BY UTILIZING PSYCHOLOGICAL OPERATIONS.**

proactive Psychological Operations, but these cannot simply be transplanting the existing and historical capabilities and trying to apply them to these newer threats. For instance, it was reported in October 2018 that U.S. Cyber Command was going on the offensive against the Russian cyber operators — military, civilian and contract — who have been targeting the U.S. and our EU and NATO allies.<sup>17</sup> The reporting indicated that our cyber operators have been sending direct messages to the Russians we seek to check, letting them know that we know who they are. While this is an important action to take, just as other more offensive and defensive cyber operations are and will continue to be, it is simply insufficient to successfully deal with the problem. Russia's weaponization of the Cyber Domain to attack the U.S. and our EU and NATO allies is not the key center of gravity in this new type of 21st Century warfare. And this strange new war we find ourselves in will not be won, because it cannot be won, simply through hacking, planting viruses and malware, and tightening down cyber security protocols to make American and allied systems more secure and resilient. It can only be won by utilizing Psychological Operations.

The key centers of gravity in this new form of war are not Russia's computers or the Internet or social media. These are the theaters of operations. Rather the key centers of gravity are Russia's leadership — specifically Vladimir Putin; the leaders of Russia's co-mingled intelligence, organized crime and wealthy oligarchs that both support his actions who are under his control; and the Russian citizenry. If we want Russia to stop what it is doing, then eroding support for the kleptocratic organized crime state that Putin is running under the label of managed democracy is both a necessary and a sufficient condition to seeing

real change. This is not to diminish the importance of both offensive cyber operations that do damage to Putin and his inner circle of oligarchs, intelligence and foreign affairs leadership, and organized crime leaders — often the same people fit into more than one of those categories — and defensive cyber operations to harden targets thereby reducing the ability of Putin to achieve his goals. These are all exceedingly important. However, the reality is that these cyber operations cannot and will not resolve the problem. What will is Letting Psychological Operators do what they do best will have the biggest impact. In this case, leveraging the Cyber Domain to deliver information for effect to change the attitudes of Russians themselves so that the corrupt, kleptocratic, organized crime state they are living in, as well as Putin's leadership of it, become intolerable to them. This is what Putin fears. It is why he has destroyed a free press. It is why he has invested so much in his attempts to demonize the promotion of civic society and good government development within the former Soviet states that Putin claims as his sphere of influence and near abroad, often centered around non-government organizations leveraged by U.S. Agency for International Development.

To hearken back to some of the doctrinal language that General Odierno liked to use when he was the Chief of Staff, part of Psychological Operations role will need to be using information for effect to shape the 21st Century Operating Environment to prevent conflict whenever possible, and when that fails to leverage that shaping to win when it is necessary to fight in the and, Sea and/or Air domains. While we normally, especially within the conventional force, talk about and understand setting the theater in terms of the physical and geographic theater; where camps, bases, and outposts,

01  
Soldiers participate in the third annual AvengerCon, a hacker-style training event, at Fort Meade, Maryland. Psychological operators must leverage the Cyber Domain as a means to deliver information for effect to change the attitudes and perceptions of targeted populations. DoD PHOTO BY STEVEN STOVER





01

phase lines and main supply routes will be placed and situated, we need to broaden that understanding for the 21st Century Operating Environment. Psychological Operations continues to have a major role to play in understanding the social behavioral nuances of both potential, actual and virtual theaters of operation. It must also continue to used to leverage the traditional Information Domain, as well as the informational components of the cyber domain, to actively set the socio-cultural and social behavioral aspects of that theater.

This is especially important given the type of conflict that has emerged over the past several years. So much of it is not taking place on regular battlefields or even by adversaries utilizing what is traditionally considered weaponry. The key battlefield of the 21st Century operating environment is the Cyber Domain and one of the two major weapon systems is Psychological Operations. If we want Russia to stop trying to rip American, British, French, German, Austrians, Greeks, Spanish and many other of our allies and partners civil societies apart, then they cannot just be deterred through offensive and defensive cyber operations. These informational threats have to be countered through offensive Psychological Operations delivered through the various information systems of the Cyber Domain. There is a need for offensive Psychological Operations to deliver information that effects actual change to Chinese and North Korean behavior. This also applies to countering the ability

for ISIS to both utilize terrorist attacks as part of a Psychological Operations strategy to get the U.S., the EU, and NATO to change their own policies, but also to utilize information for effect to prevent ISIS from radicalizing parts of the Muslim minority communities in the U.S. and our EU and NATO partners into weapons.

The Psychological Operations community also has an important defensive role to play. The nebulous nature of this 21st Century theater of operation requires senior leaders in the U.S. military and the Interagency to engage with the Psychological Operations community to develop a 21st Century form of counter-Psychological Operations. As important as it is for the U.S. military to be expeditionary, to be out in the world engaging with our allies and partners and peer competitors, it is as important to respect the Posse Comitatus Act and limit U.S. military operations within the U.S. to times of genuine emergency, much of the conflict so far in the 21st Century Operating Environment cannot be neatly divided into continental versus outside the continental U.S. New rules of engagement and accommodations for how, when, and where Psychological Operations, as a weapons system to counter these 21st Century threats, must be developed. The members of the Psychological Operations community are the American subject-matter experts on using information for affect in order to influence the emotions, motives, objective reasoning, and ultimately the behavior of foreign governments,

01  
Brig. Gen. Khalil Essam Mohamed Elsayed, commander, Egyptian Human Development and Behavioral Sciences Center, listens intently as a 4th Psychological Operations Group Soldier explains the capabilities of the group's graphics section during a visit to Fort Bragg, North Carolina. Information exchange, in order to coordinate training programs and synchronize efforts with NATO allies and other partners is an important factor that will help shape the battlefield of the 21st Century operating environment.

U.S. ARMY PHOTO BY STAFF SGT. KISSTA DIGREGORIO



02

organizations, groups and individuals.<sup>18</sup> There is no one better to turn to now than the Psychological Operations community to combat both the great power and non-state threats that seek to leverage both the cyber and terrestrial domains to deliver information to effect American behavior, as well as of our EU and NATO allies and partners. Your expertise in developing and delivering those simple appeals, to use Fall's formulation, to increase our resiliency to withstand and ward off the signals and messages and ideas directed at us and our allies is essential to successfully emerging from this new era of great power and non-state actor competition.

The expertise-based contributions of the Psychological Operations community extend beyond just offensive and defensive operations. It is also necessary to leverage the power of providing information for effect to maintenance of the steady state in the 21st Century Operating Environment so that it does not become an overgrown garden. As Hannah Arendt explained in *The Origins of Totalitarianism*:

*The ideal subject of totalitarian rule is not the convinced Nazi or the dedicated Communist, but people for whom the distinction between fact and fiction (i.e. the reality of experience) and the distinction between true and false (i.e. the standards of thought) no longer exist.*<sup>19</sup>

In the 21st Century Operating Environment, especially in this new 21st Century War of Ideas, Psychological Operations are a powerful tool in both shoring up the distinction between fact and fiction, between true and false, as well as ensuring that we can all tell the difference. 

## ABOUT THE AUTHOR

**Adam L. Silverman** has a doctorate of philosophy in political science and criminology from the University of Florida (2002) and is currently a National Security Consultant with Helios Global, Inc (2015-Present). He has previously been a Senior Fellow at JSOU (2015), a subject matter expert with the Office of the Secretary of Defense for Security Dialogue and U.S. Army Europe (2014), the Cultural Advisor (TACON) at U.S. Army Europe (2013-2014), the Cultural Advisor (TACON) at CA Branch (2014), the Cultural Advisor (TACON) III Corps (2012), the Cultural Advisor at U.S. Army War College (2010-2014), and the Cultural Advisor for the 2nd Brigade Combat Team/1st Armored Division (2007-2008) deployed with the BCT in Iraq in 2008. Dr. Silverman has also provided support for numerous Army, DoD, and Interagency elements.

02

**A Solider monitors exercise progress during a cyberspace training scenario. One of the key 21st Century theaters of operation is cyberspace. Unlike the more traditional theaters of operations, cyberspace is everywhere and nowhere all at the same time. The nebulous nature of this 21st Century theater of operation requires senior leaders in the U.S. military and the Interagency to engage with the Psychological Operations community to develop a 21st Century form of counter-Psychological Operations. U.S. ARMY PHOTO BY BILL ROCHE**

**NOTES** 01. This essay is adapted from the keynote address delivered at the Psychological Operations Regiment's 100th anniversary regimental dinner, November 3, 2018. 02. Robert Gerwarth, *The Vanquished: Why the First World War Failed to End* (Farrar, Straus, and Giroux, 2017). 03. Karen Darwisha, *Putin's Kleptocracy: Who Owns Russia?* (Simon and Schuster, 2015). 04. James A. Schnell, "Attributing Strategic and Global Reach Within a Cross-Cultural Understanding of the Chinese 'Belt and Road Initiative,'" *Fudan Journal of the Humanities and Social Sciences*, 17 FEB 2018. 05. Adam L. Silverman, *The Need to Revisit U.S. Policy in the Middle East: The Islamic State's Doctrine and its Use of Terrorism as Psychological Operations*, Helios Global Analytical Report prepared for MG A. Ray Royalty, Headquarters Department of the Army, G34/Force Protection, December 2015. 06. *The National Security Strategy of the United States*, The White House, December 2017. 07. Bernard Fall, "The Theory and Practice of Insurgency and Counterinsurgency," *Naval War College Review*, Winter 1968, reprinted in *Military Review*, September-October 2015, [https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview\\_20151031\\_art009.pdf](https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20151031_art009.pdf). 08. Schnell, February 17, 2018. 09. "World's Largest Economies," *CNN Money*, January 18, 2018, [https://money.cnn.com/news/economy/world\\_economies\\_gdp/index.html](https://money.cnn.com/news/economy/world_economies_gdp/index.html). 10. Ivana Kottasova, "Russian Military Spending Drops for the First Time in 10 Years," *CNN Money*, May 2, 2018, <https://money.cnn.com/2018/05/02/news/russia-defense-spending-plunge/index.html>. 11. David Mujamdar, "Russia's Only Aircraft Carrier Will Get New MiG-29s," *The National Interest*, August 18, 2018, <https://nationalinterest.org/blog/buzz/russia%E2%80%99s-only-aircraft-carrier-will-get-new-mig-29s-28097>. 12. David Sanger, "Hack of Saudi Petrochemical Plant Was Coordinated From Russian Institute," *The New York Times*, October 23, 2018, <https://www.nytimes.com/2018/10/23/us/politics/russian-hackers-saudi-chemical-plant.html>. 13. Luis Gomez, "Exactly How Much Russians Spent on Twitter, Facebook Ads During Election," *The San Diego Union Tribune*, September 28, 2017, <http://www.sandiegouniontribune.com/opinion/the-conversation/sd-how-much-money-russians-spent-twitter-facebook-ads-20170928-htmlstory.html>. 14. Gregg Miller and Soaud Mekhennet, "Inside the World of the Islamic State's Propaganda Machine," *The Alaska Dispatch News*, November 20, 2015, <http://www.adn.com/article/20151120/inside-surreal-world-islamic-state-s-propaganda-machine>. 15. Melissa K. Byrnes, "Solidarity and 'Je Suis Paris,'" *Lawyers, Guns, and Money*, November 15, 2015, <http://www.lawyersgunsandmoneyblog.com/2015/11/solidarity-and-je-suis-paris>. 16. Silverman, December 2015. 17. Julia Barnes, "U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections," *The New York Times*, October 23, 2018, <https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html>. 18. *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms*. 19. Hannah Arendt, *The Origins of Totalitarianism*, (Harcourt, Brace, Jovanovich, 1973).