Submission: 2018 International Conference on Cyber Conflict, CyCon US, "Cyber Conflict During Competition" (submitted July 2018)

"Strategic Cyber: Responding to Russian Online Information Warfare"

by Matthew J. Flynn, PhD

Abstract: The success of the democratic world and its citizens depends to a great extent on recognizing one's strategic advantages. Secure on this high ground, a nation can dictate the inter-state strategic competition in favor of US national security. In cyberspace that advantage rests on defending and advancing a US ideological advantage inherent in that platform. The quality of openness ensures a confrontation unfolding well short of armed conflict and winning that war matters most to those seeking to erode this US strategic ascendancy. This paper follows Russia's progression in its effort to reverse its unfavorable situation in cyberspace, largely by hoping to panic the United States into a series of poor policy decisions. A failure to see openness as the means to thwart this cognitive offensive all but hands Russia a victory. Reversing this outcome stands to blunt cyber tensions from giving rise to a means of setting conditions for a fait accompli *and a military clash of arms. With this end in mind, there is much reason for optimism at the strategic level of such a war in cyberspace.*

Matthew J. Flynn, PhD., is Professor of War Studies at Marine Corps University, Quantico VA. He specializes in the evolution of warfare and has written on topics such as preemptive war, revolutionary war, borders and frontiers, and militarization in the cyber domain.

Perhaps no state has grasped the implications of cyberspace to foster political activism more than Russia. In 2007, and again in 2008, popular expression online helped propel Russia into conflict with its neighbors, first in Estonia in the Baltic region, and then in Georgia to the southeast. In both cases, the power of internet access challenged the Russian government's ability to dictate events. By 2014, strongman Vladimir Putin no longer feared the unintended consequences of that platform and could in fact look to capitalize on that technology to spur unrest in other countries, an effort that climaxed with the hack of the US presidential election in 2016. Even so, Russia remains at a severe disadvantage in cyberspace because that domain, while a new arena, reinforces an old military truism—it is best to enjoy the strategic high ground

in any conflict. Russian actions in cyberspace reveal a state trying to achieve this favorable dynamic and almost succeeding with the unwitting help of the United States. This paper exposes Russia's effort to reverse its strategic weakness in cyberspace by restricting internet access out of fear that a community of users there can threaten the legitimacy of centralized government within Russia. The Kremlin's attempts to curb this online presence should serve as a reminder of the importance of supporting the existing US cyber policy of defending and advancing an open internet to hold onto the strategic high ground in cyberspace.[1]

CYBER IDEOLOGY

For Russia, controlling online access is less about shaping the battlespace for the next war and more about accepting the ideological showdown that the internet imposes upon restrictive governments. This cognitive struggle unfolds below a threshold of violence coming at the hands of armed conflict that usually serves to define war. Russia seized upon this construct to better position itself globally in the ether of cyberspace. It did so, however, only after a painful trajectory that witnessed online users threaten the authority of the state. In fact, regimes hostile to representative governmental norms had to weather the changes stemming from these cyber rebellions and then learn how to discredit them. This reaction made clear the tangible threat that openness poses to nations fearing the quality of shared space producing an online community which clearly embraced the democratic values of connecting people and sharing

[1]. The US cyber policy defending and advancing openness rests on a series of public documents. See "The International Strategy for Cyberspace," White House, May 2011; Department of Defense, "Strategy for Operating in Cyberspace," July 2011; Department of Defense, "Cyber Strategy," April 2015; Department of State, "Cyber Strategy," 2016, and from the Trump administration, Presidential Executive Order, "Cyber Security," May 11, 2017.

information and doing so free of oversight from governing bodies. That dynamic ensured that online connectivity became a means of challenging authoritarian regimes through cyberspace.[2]

This analysis covers three main events to evidence the Russian trajectory to combat this threat and find safe footing in cyberspace. The cyber wars first in Estonia in 2007, then Georgia in 2008, yield to an examination of Russian efforts at home and then in Crimea and Ukraine. This progression not only underscores the ideological dimensions of the standalone cyber war, but also stresses the lack of awareness of this dynamic by the United States. The piece ends by stressing the strategic ascendancy the United States enjoys in the cyber domain and offers some suggestions for maintaining this advantage. In this way, the analysis turns state competition in cyberspace into a valued context revealing how a cognitive cyber offensive can expand user access in cyberspace and help usher in a new era of containment that, as in the Cold War, confronts US adversaries with the losing proposition of thwarting basic human values. This ideological aspect of cyberspace places foes of openness on the defensive, impeding war long before it reaches a *fait accompli* campaign settled primarily with conventional forces.

Following this Russian progression of waging war in cyberspace recasts a portion of the familiar narrative of Russian online actions seamlessly interfacing with its military efforts. In fact, those addressing Russian actions in Estonia and Georgia note the gap between action and

---

[2]. John Arquilla highlighted this potentiality early on. See Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, Vol. 12, No. 2 (Spring 1993): 144,145. Martin C. Libicki said something similar when examining what he called "friendly conquest," or ideologically driven conflict over values online. See Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (New York: Cambridge University, 2007), 4, 230. Many authors withhold judgment on whether mere connectivity can force authoritarian regimes to liberalize given the success of strongmen using the internet to augment state oversight thus far. See Jay Blumler and Stephen Coleman, *The Internet and Democratic Citizenship: Theory, Practice and Policy* (New York: Cambridge University, 2009), 9; Larry Diamond, "Liberation Technology," *Journal of Democracy,* Vol. 21, No. 3 (July 2010): 70; and recently, Vincent Mosco, *Becoming Digital: Towards a Post-Internet Society* (Bingley: Emerald Publishing, 2017), 14.

effect even as they validate that coordination.[3] This conclusion greatly overstates their efficacy as is made clear below. Too often, cyber connectivity worked against Russian authorities at home, but that outcome simply goes unacknowledged by those weighing the military implications of Russia's use of cyberspace. Yet the concern about divisions at home is prominent in the scholarship examining Putin's effort to maintain his power and this point is also made plain in this analysis. Omitting this context skews any understanding of Russian fear as a motive for acting in cyberspace, a failure that warps US policy efforts to counter the threat. In particular, Russia's hack of the US 2016 presidential election has prompted a US defensive effort in cyberspace, surrendering cyber ideology as the attack vehicle it is. To regain the strategic high ground derived from cyber rebellions requires a conscious effort by US decision makers to ensure that a free exchange of online messaging gets into the cyberspace of those seeking to thwart this end.

One stops short of labeling this online political activism a revolution because that word suggests outcome more than process, and a focus on process is key. From this viewpoint, a revolution births a movement while rebellions merely embrace a possible change, something that may or may not come to pass. Cyber rebellions point to realities in cyberspace that could lead to

---

[3]. For Estonia, see Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts During the Internet War," *Georgetown Journal of International Affairs*, Winter/Spring 2008: 123; Robert A. Miller and Daniel T. Kuehl, "Cyberspace and the 'First Battle' in 21st-century War," *Defense Horizons*, No. 68 (September 2009): 3; Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: HarperCollins, 2010), 16; *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2010), 23; Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security*, Vol. 4, No. 2 (Summer 2011): 51; and Alison Lawlor Russell, *Cyber Blockades* (Washington, DC: Georgetown University, 2014), 86. For Georgia, see *Cyber Attacks Against Georgia: Legal Lessons Identified* (Tallinn, Estonia: Cooperative Cyber Defense Center of Excellence, 2008): 9-10, 12; *International Cyber Incidents,* 75-76; Clarke and Knake, *Cyber War,* 20; Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review* (November-December 2011): 63-64; Russell, *Cyber Blockades*, 105.

an ideological gain for states embracing openness. The term recalls what once was and the imperative to get it back. Reminding US policy makers that those opposing democracy face a threat from this medium is the main purpose here and one best seen in the Russian response to this threat. Getting cyber right goes a long way to validating current US policy as defending and advancing openness. As one journalist recently wrote, cyber is a "perfect weapon" to fray combustible civic bodies, although that individual meant liberal societies.[4] The United States must carry that fight to the Russian body politic and do so by fostering a global online community. That task suffers as the United States retreats from demanding openness online, best seen in the alarming tendency of experts to call for a new cyber strategy to better serve US interests. That pronouncement implicitly accepts cyber sovereignty and accedes to the hope of US adversaries to enforce national borders in cyberspace and thereby blunt the impact of connectivity.[5] A look at Russia's struggles with online activism underscores the need for openness in order to enable nations welcoming an online exchange to profit from the ideological utility of the cyber domain.

ESTONIA: Caught by Surprise

The Russian attack on Estonia appeared far short of an act of war and looked to consist only of a cyber disruption and nothing more. There is no evidence of a congruent purpose, such as a ground attack, and this cyber incident most likely substituted for such retaliation. In this sense, the cyber territory mitigated conflict by offering a new outlet for expressing a foreign policy grievance. Many Russians certainly felt that Estonia had authored such an affront when in

---

4. David E. Sanger, *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age* (New York: Crown, 2018), xv-xvi.

5. Advocates of a cyber Westphalian norm do the most damage in this regard, appealing to the establishment of national borders in Europe in 1648, a development that fed authoritarian rule. See Chris C. Demchak and Peter Dembrowski, "Rise of a Cybered Westphalian Age," *Strategic Studies Quarterly* (Spring 2011): 35, 37.

late April 2007, after considerable public debate, the state sanctioned removal of a statue commemorating Soviet dead who had fought to liberate Estonia from Nazi control during the Second World War. To most Estonians, the statue represented Russian occupation not liberation. Moreover, citizens of the Baltic nation believed the statue served as a rallying point for extremists among Estonia's considerable number of ethnic Russians totaling a quarter of the country's population. As the removal became imminent, radicals in that group helped foment riots in Estonia's capital, Tallinn.[6] These disruptions ceased after a few days and by April 30 the statue was installed at the Tallinn Military Cemetery.

Outrage may not have gone further than this had it not been for the internet. The Russian-language blogosphere and online Russian forums fueled popular discontent to the point of encouraging all Russians so offended, those in Estonia and beyond its borders, to take matters into their own hands and strike back online.[7] There concerned citizens could find prompts to launch ping-flooding and malformed queries to enable them to execute an "attack" on Estonia and conceivably shut down the internet in many of its cities.[8]

The response was rapid and overwhelming. Soon, this Russian popular front reduced Estonian bandwidth, crashing the websites of numerous government ministries and a few major banks. Notably, the attacks avoided power grids and water supply facilities, although the attacks demonstrated the potential to do just that.[9] The harmful traffic intensified on May 9, the day that marked the anniversary of the end of Russia's involvement in World War II. Specialists in the

---

6. *International Cyber Incidents*, 16; Evron, "Battling Botnets and Online Mobs," 122; and Russell, *Cyber Blockades*, 75.
7. *International Cyber Incidents,* 23; and Herzog, "Revisiting the Estonian Cyber Attacks," 51.
8. *International Cyber Incidents,* 20; Russell, *Cyber Blockades*, 75; and Evron, "Battling Botnets and Online Mobs," 123.
9. *International Cyber Incidents,* 21; Herzog, "Revisiting the Estonian Cyber Attacks," 52.

employ of the Estonian government curbed this flow and did so by ordering some victims to unplug, thereby imposing a "self-blockade" on Estonia.[10] The incidents dissipated shortly thereafter, although a few more waves occurred in subsequent days. During the three weeks of attacks most Estonians experienced some service interruption. In this respect, the spontaneous Russian initiative appeared to have met its goal of disrupting the "most wired nation in Europe," as *Wired Magazine* labeled that country due to its purposeful reliance on cyberspace.[11]

If the Russian intent was clear, the motives were less so. What was gained by the attack? What had been achieved? Yes, some Estonians could not function normally for a number of days, but the Estonian authorities did not return the statue to the town center. Still, Russian pride had been assuaged and this satisfied the main purpose. The Russian citizenry had employed a "cyber riot" to lash out and avenge a wrong and did so without violence.[12] A popular protest had rebuked a neighbor, and one could not but acknowledge what it was: A true expression of democracy. This was all the more true because government sanction of the event did not come to the fore. In this instance, attribution was unclear, but only at the end of the chain. Certainly, populism had sent Russians to their computers where a hacktivist community assisted their efforts. But were the hacktivists working at the behest of the state? This was not clear, nor has the Russian government ever claimed responsibility, with one Russian statesman publicly denouncing the attack as "cyber-terrorism."[13] This label is most telling, not in underscoring the challenges of attribution, real as they are, but in stressing this incident as one of democratic

---

10. Russell, *Cyber Blockades*, 79.
11. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine*, Issue 15.09, August 21, 2007.
12. Evron, "Battling Botnets and Online Mobs," 123.
13. Herzog, "Revisiting the Estonian Cyber Attacks," 54; Evron, "Battling Botnets and Online Mobs," 124. The Russian Deputy Press Secretary Dmitry Peskov called the attack an act of terrorism. See Russell, *Cyber Blockades*, 82.

activism. This ideological purpose had become plain in a country hardly known for its democratic tradition. In fact, the opposite had been the norm, authoritarianism plaguing Russia's history from Czars to Communist thugs, and even to the current appearance of *imperium* at the highest levels of government in the person of Vladimir Putin.[14] In defiance of this history, the internet had enabled Russian citizens to achieve what they had not been able to do over hundreds of years, and that was demonstrate an outgrowth of popular expression independent of any government control. It was a phenomenal moment.

No one noticed. Russian failures to make more of this success are perhaps understandable. They could not dig themselves out from under the weight of their history, so a healthier democracy was not forthcoming. While the state boasts a large and talented pool of hackers brandishing tremendous technological prowess, that capability appears to lie outside any shared ideological purpose.[15] The technology can stand on its own. If this view is endemic to a hacker mentality, and if this view is indicative of an ideological purpose that is more instinctive than institutional in Russians, the strike on Estonia leaves Russia pioneering cyber warfare as an ideological weapon, but not realizing this is so.

Ironically, the same can be said of Western powers. The ideological purpose of advancing democracy globally is a longstanding concern of Western nations, particularly the United States. This goal was advanced by Russia when attacking Estonia, yet the West saw no such success, only fear of motives. Russia attacked Estonia to probe NATO's response when it

---

[14]. William Zimmerman, *Ruling Russia: Authoritarianism from the Revolution to Putin* (Princeton, NJ: Princeton University, 2014), 2. The Russian people acquiescing to authoritarianism is in Richard Pipes, "Flight from Freedom: What Russians Think and Want," *Foreign Affairs* 83, 3 (May-June 2004): 15; and Gregory Feifer, *Russians: The People Behind the Power* (New York: Twelve, 2014), 8.

[15]. Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," CNA (March 2017): 10.

came to a battle to control cyberspace.[16] With cyber supremacy, a conventional military strike could follow.[17] These were valid concerns and needed close attention given attribution issues, for it remained unclear whether a popular movement could execute a distributed denial of service attack (DDoS), one which needed a legion of hijacked computers turned into botnets to succeed.[18] Only a carefully coordinated attack could marshal this resource to its greatest effect. So the question still looms: Was the Russian government behind the attacks? Here the West's old fear of Soviet secrecy arose anew. Had the security arm of the Russian government today, the Federal Security Service of the Russian Federation (FSB), having taken over for its Cold War version, the KGB, orchestrated the attacks in league with criminal organizations?[19]

Should this be true, what transpired in Estonia meant the Russian government tested a tool of espionage that lay very close to an act of war should the intent be overtaken by popular elements online. In this sense, some deniability made sense to ensure cyber disruption did not appear to have state sanction, for that admission could raise tensions leading to an outbreak of warfare on the ground. But deniability raised another unsettling question. What if the Russian government could not control criminal elements within the state and they had acted independently? Here was a dangerous precedent, private actors taking matters into their own hands. But to what end? What gain would criminals enjoy in this instance? Since answers were not clear, thinking rests in larger part on the ideology of the attack – that even criminals agreed

16. Herzog, "Revisiting the Estonian Cyber Attacks," 55; Häly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, Issue 63, 4th Quarter (2011): 60.
17. E. Lincoln Bonner III, "Cyber Power in 21st Century Joint Warfare," *Joint Force Quarterly*, Issue 74, 3rd Quarter (2014): 103.
18. A botnet refers to computers marshaled together via the internet and answerable to an individual who forwards transmissions usually without the owner's awareness. A DDoS or distributed denial of service attack uses compromised systems and often botnets to overwhelm a targeted system.
19. Andrei Soldatov and Irina Borogan, *The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB* (New York: Public Affairs, 2010), 238, 3.

to salvage some national pride and take part in the strike. But the thinking has not gone that far. The implications of a democratic impulse sweeping Russia and pulling criminals in that direction resulting in a patriotic cyber attack, and such a spectacle blooming overnight, independent of the state, went unacknowledged in the West.

GEORGIA: A Dangerous Sequel

The cyber war in Estonia remained a muted affair, solely an online confrontation. Still, the fact remained that renegade online fronts sparked this crisis by unleashing cyber attacks on Estonia and did so independent of the Russian government even if given its tacit approval and later its encouragement. This meant that openness had hit a threshold where state control could not curb public discontent expressed online. This democratic movement assumed uncertain dimensions within the Russian state as growing authoritarian rule faced spontaneous challengers.

This experience in Estonia helped pull Russia into another confrontation the following year, this time with the country of Georgia in the Caucasus region. The former Soviet republic had asserted its independence in 1991 in the wake of the collapse of the USSR. But two territories within that state, South Ossetia and Abkhazia, mustered a counter action and Russians living within those territories separated themselves from Georgia. An uneasy standoff ensued, with Georgia maintaining the right of control there, even as Russians in both places looked to Moscow. In July 2008, the separatists in South Ossetia launched a series of missile raids on nearby Georgian villages. Georgia retaliated with ground forces on August 7. The Russian military immediately responded and quickly engaged Georgian troops the next day. Further Russian attacks came in Abkhazia. In five days, Russian assistance meant that Georgia was cast

out of both South Ossetia and Abkhazia, losing some Georgian territory as well. A détente was reached with Russian backing of the two territories as independent of Georgian rule.

Russian online activity preceded the ground attack by a day, initially in something of a trivial fashion as Russian actors in cyberspace defaced websites of the Georgian state, including doctoring images and likening Georgian president Mikheil Saakashvili to Adolf Hitler.[20] Observers correctly highlighted the more serious elements of the cyber attack such as striking out at Georgian government websites, the banking system, news outlets and online discussion forums as an aggressive means to isolate the country from outside contact.[21] These actions helped a Russian media blitz justifying the legitimacy of the Russian ground attack. Strategic messaging also spoke to Russian success in impacting the command and control of Georgian forces.[22] In a week, Russia had pioneered a new way of fighting by teaming cyber capabilities with a conventional attack.[23]

The timing of the cyber attacks to coincide with the Russian ground attack indicates a carefully coordinated strategy. But cyber actions were underway a month before the ground attack.[24] One could view this as necessary reconnaissance to prepare the cyber offensive and then the ground attack. That probing certainly suggested a looming attack, all but forfeiting surprise and alerting the target to its danger. In this light, the Russian ground offensive on August 8 did not represent a planned date of attack, but a point of no further recourse other than to attack, in order to take advantage of the very real cyber disruption already ongoing in Georgia and soon to be readily apparent to the outside world. While long expecting a confrontation with Georgia,

---

20. Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," 64; *Cyber Attacks Against Georgia,* 7-8.
21. *International Cyber Incidents,* 70.
22. Miller and Kuehl, "Cyberspace and the 'First Battle' in 21st-century War," 2, 5.
23. Miller and Kuehl, "Cyberspace and the 'First Battle' in 21st-century War," 1, 2.
24. Miller and Kuehl, "Cyberspace and the 'First Battle' in 21st-century War," 3; *International Cyber Incidents,* 69.

Russian leadership was caught off guard by the timing of hostilities.[25] Russian planners had to incorporate the cyber element into the offensive both to gain military advantage and to head off the potential of a public presence online to impede those plans and take things in an unwanted direction.

The success in controlling the online elements was mixed. Youth groups again went into action and, in the name of patriotism, targeted specific websites. Much of this traffic had Russian sponsors co-opting this online movement.[26] More telling was suspicion that criminal organizations answered the Russian government's call to action and engaged in the familiar DDoS attack.[27] The Russian government disavowed these actors, again taking advantage of attribution difficulties to disguise the fact that the government had been blindsided by the chaos unfolding online. Even if teaming with such actors, the need to have to look to such unreliable online partners risked throwing the military plans into potential disarray. The message here was not that Russia had unleashed a devastating military attack, but that its online community was impacting the foreign policy actions of a government forced to keep pace with this new online offensive. This became more visible when cyber attacks continued after the cessation of ground operations, as the Russian online community took the lead using forums, blogs and websites.[28]

Despite efforts at control, Russian cyber attacks could not stop Georgians from blogging, detracting considerably from the Russian effort to enjoy information dominance over the

---

[25]. Andrei Illarionov asserts that Russia acted on a plan in place for ten years. See Illarionov, "The Russia Leadership's Preparation for War, 1999-2008," in *The Guns of August: Russia's War in Georgia*, eds. Svante E. Cornell and S. Frederick Starr (New York: Routledge, 2015), 50. For Russian leadership being surprised by the timing of hostilities, see Ariel Cohen and Robert E. Hamilton, *The Russian Military and the Georgian War: Lessons and Implications*, Strategic Studies Institute, US Army War College, Carlisle, PN (June 2011), 22, 23.
[26]. "Russia/Georgia Cyber War – Findings and Analysis," Project Grey Goose, Phase I Report (17 October 2008): 6-8.
[27]. Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," 64; and Russell, *Cyber Blockades*, 109-110.
[28]. *International Cyber Incidents,* 68, 71.

battlefield.[29] Other failures to isolate the cyber battlefield threatened to escalate the conflict. Most significantly, Georgia, in response to the cyber attacks, shifted access to a server based in the state of Georgia in the United States, without US government approval. The Russian aggressors online followed them there.[30] Now, a border dispute in the Caucasus region threatened to include an offensive cyber action on American soil. How should the United States respond? Furthermore, Georgia was pursuing membership in NATO and a Russian attack could have triggered a response from that organization, thereby escalating the local conflict. But NATO had not responded in that fashion when Estonia, an alliance member, experienced its cyber attack, member states deciding that the strike did not amount to an attack.[31] The possibility of NATO acting in the case of Georgia over just cyber events was remote, but a ground attack could provoke a different response.

The last thing Russia wanted was a clash with NATO.[32] Disarray after the Soviet Union's demise left Russian military forces in marked decline both in quality and capability. The First Chechen War exposed these shortcomings and not much had changed almost two decades later.[33] Still, a naval action as well as air assets accompanied the attack on Georgia, and this joint force spoke to some Russian vitality of arms. But the need to supplement the district forces with outside specialized units further stoked the fear that a military action could flounder given the poor state of Russian arms. Those planning the attack employed overwhelming numbers with

---

29. Paul A. Goble, "Defining Victory and Defeat: The Information War Between Russia and Georgia," in *The Guns of August: Russia's War in Georgia*, eds. Svante E. Cornell and S. Frederick Starr (New York: Routledge, 2015), 191.
30. Stephen W. Korns and Joshua E. Kastenberg, "Georgia's Cyber Left Hook," *Parameters* (Winter 2008-2009): 60; and *International Cyber Incidents,* 70, 77.
31. Häly Laasme, "Estonia: Cyber Window into the Future of NATO," *Joint Force Quarterly*, Issue 63 (4th Quarter 2011): 60.
32. Herzog, "Revisiting the Estonian Cyber Attacks," 53.
33. Zoltan Barany, *Democratic Breakdown and the Decline of the Russian Military* (Princeton, NJ: Princeton University, 2007), 95, 99-100.

30,0000 Russian troops double that of the Georgian military.[34] The clash that followed needed to be brief to avoid triggering adventurism in countries along Russia's periphery. The struggle in Chechnia had devolved into an ugly guerrilla war that included acts of terrorism in Russia itself, plunging the Russian home front into discord. Having another protracted border dispute on its hands in 2008 could well cripple Russian efforts to recover from the 1991 collapse.

The good news of a very short, limited conflict in Georgia was dampened by more troubling developments when the cyber element of the clash is considered. A close look at the cyber events surrounding the Russian attack on Georgia presented observers with a Russian reaction to online activity it strove to control, rather than a carefully planned test of future war in the hands of a sophisticated Russian army. Theoretically the two purposes could coexist. Russia could test its ability to use cyber attacks in conjunction with conventional force. A formal Russian military response followed a barrage of online attacks on Georgia, signaling an evolutionary step in warfare as kinetic force teamed with cyber actions designed to prep the invasion. This synergy certainly defined events in Georgia, but alarmed Western observers then missed the key, related significance of that episode. The foreign policy goals of the Russian state would be set by its government, not by popular mandates online enabled by a handful of computer adventurers. That activism smacked of populism in far too clear a way to be tolerated. Russian intervention in Georgia cemented resolve among the leadership to get control of the patriotic hackers so markedly unrestrained in this domain.

To achieve this end, the risk of a larger war was worth it. For Russia, the main struggle was heading off democratic movements in neighboring territories. Georgia had endured this fate

---

[34]. For the Russian order of battle, see Cohen and Hamilton, *The Russian Military and the Georgian War*, 10; and Pavel Felgenhauer, "After August 7: The Escalation of the Russia-Georgia War," in *The Guns of August: Russia's War in Georgia*, eds. Svante E. Cornell and S. Frederick Starr (New York: Routledge, 2015), 166-167.

in late 2003 with the Rose Revolution that brought Saakashvili to power. A year later, vast public protests deposed the leader of Ukraine during the Orange Revolution and a year after that the leader of Kyrgyzstan with the Tulip Revolution. Putin's antipathy for Saakashvili underscored his determination to humble all instances of these "Color Revolutions."[35] By 2008, Putin, now prime minster, helped orchestrate Russian military action against Georgia.[36] But that strike failed to topple his rival and in at least one way made matters worse. Encouraging separatists abroad invited such dissidence to spill over into Russia.[37] An activist cyber element compounded that risk, and blunting that online presence to help shore up the homeland would come next.

CONSOLIDATION: 2008-2014

The events in Estonia stress that openness had fostered a rogue element within Russian politics that acted by its own compass and initiated Russian cyber actions against that Baltic state. What transpired in Georgia just over a year later reflects the Russian government's endeavor to tailor online realities in favor of state authority, with imperfect results. After 2008, this aim became Putin's aim. Having given up the presidency, he looked to stay in charge in a state which ostensibly curtails such permanence. Operating in elite circles, he overwhelmed his peers in government, manipulating state offices and the personnel holding those offices.[38] Such

---

[35]. Lincoln A. Mitchel, *The Color Revolutions* (Philadelphia, PN: University of Pennsylvania, 2012), 113.
[36]. Ronald D. Asmus, *A Little War that Shook the World: Georgia, Russia, and the Future of the West* (New York: Palgrave Macmillan, 2010), 179.
[37]. Goble, "Defining Victory and Defeat," 190. See also Angela Stent, *The Limits of Partnership: US-Russian Relations in the Twenty-First Century* (Princeton, NJ: Princeton University, 2014), 101, 115; Fiona Hill and Clifford G. Gaddy, *Mr. Putin: Operative in the Kremlin* (Washington DC: Brookings Institution Press, 2013), 343; and Roger N. McDermott, "Learning from Today's War: Does Russia Have a Gerasimov Doctrine?" *Parameters*, Vol. 46, No. 1 (Spring 2016): 99, 101.
[38]. For elites dominating Russian political fortunes and Putin manipulating such factions, see Vladimir Gel'man, *Authoritarian Russia: Analyzing Post-Soviet Regimes Changes* (Pittsburgh, PA: University of Pittsburgh, 2015), xiv, 150; and Arkady Ostrovsky, *The Invention of Russia: From Gorbachev's Freedom to Putin's War* (New York: Viking, 2015), 8.

politicking was an obvious step away from robust democracy as was the next, related effort. The public also had to accept a strongman, or at least centralized power in one office. But in this case, the Russian inclination to gravitate to personality rather than process and favor authoritarianism collided with online capabilities offering to blunt this sentiment. That Russia could change from the old ways to the new came face to face with the openness defining cyberspace.

Putin already felt threatened by public demonstrations that in his view had helped West Germany absorb East Germany starting a reaction that eventually destroyed the Soviet Union.[39] Indeed, protests had surfaced in Russia as he plotted his return to the presidency in 2012. On December 10, 2011, Russians rallied against fraudulent parliamentary elections during the Snow Revolution. On May 6, 2012, large crowds protested Putin's pending inauguration as president the next day with the March of Millions.[40] Once regaining that office, Putin cracked down on such groups within Russia. The Duma allowed the targeting of foreign groups that had accepted outside money. Russian government spokesmen tied any protests to Western influence coming from organizations such as USAID or NGOs and so-called liberal outlets were harassed by government operatives.[41]

The internet age complicated matters because opposition groups within Russia enjoyed an online presence, a sign that traditional adherence to government decree was suspect in the extreme. Social media played a leading role in posing an internal threat, helping independent organizations manipulate people into street demonstrations.[42] To rebuff what was no less than

---

39. Hill, *Mr. Putin,* 363; and Steven Lee Myers, *The New Tsar: The Rise and Reign of Vladimir Putin* (New York: Alfred A. Knopf, 2015), 48.
40. Mischa Gabowitsch, *Protest in Putin's Russia* (Polity, 2017), 8, 38.
41. Hill, *Mr. Putin,* 348; and Richard Sakwa, *Putin Redux: Power and Contradiction in Contemporary Russia* (New York: Routledge, 2014), 169, 181.
42. Hill, *Mr. Putin,* 349; Stent, *The Limits of Partnership,* 100, 101.

Western interference in Russia's internal affairs, the Kremlin had to act: Internet use had to be controlled, dissent relabeled slander and libel and therefore a criminal act, and websites were blacklisted then blocked.[43] These measures underscored Putin's desperation to crack down on the internet, something he publicly labeled no more than a CIA project in April 2014.[44] When National Security Agency (NSA) contractor Edward Snowden released NSA classified information starting in June 2013, he exposed some of that agency's online surveillance efforts and helped Putin justify his actions.[45]

The Russian government's ability to shore up things at home still did not address how connectivity aided what in Putin's mind amounted to fifth columns that imposed a democracy beholden to Western interests on Russia's neighbors.[46] Putin responded with his own Color Revolutions. To this end came a government-led campaign extolling a pure Russian identity based on true Russian cultural values. Russia could go on the offensive and do so by the means of a "Eurasianism" ideology announcing values as the key weapon to reassert a Russian-led heartland.[47] Russia had its own story to tell in this regard, as a nation long beleaguered by Western threats and actions. In this respect, the information battle ground was a key asset: A means to sow discord within states by reinforcing prejudice and bias among diverse populations that would rally to Russia because of a shared persecution.

Russia brazenly tested this approach by orchestrating a takeover of Crimea in the name of supporting an indigenous revolt of ethnic Russians against Ukrainian rule in February 2014. No matter widespread dissension and a tangible groundswell in favor of Crimea joining the Russian

---

43. Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (New York: PublicAffairs, 2015), xi.
44. Hill, *Mr. Putin,* 349.
45. Myers, *The New Tsar,* 441.
46. Hill, *Mr. Putin,* 348.
47. Myers, *The New Tsar,* 445-446.

Federation, Russian military forces, albeit minus any uniform markings or identification, proved decisive.[48] Ukraine faced the prospect of armed confrontation with para-Russian forces and chose not to engage. The ensuing information campaign by Russian authorities merely announced the supposed proclivity of Crimea to seek separation from Ukraine and then demand annexation to Russia. These two outcomes came to pass rapidly and by March 2014, Ukraine had lost control of that province. Putin then proclaimed a triumph of nationalism and the Russian public accepted the results as a measure of ancient Russian suzerainty in the region at the expense of Western interference.

Ukraine's renewed internal political turmoil had opened the door to this Russian adventurism in Crimea. Ukraine's Euromaidan reaction of February 2014 deposed the current president who favored closer ties with Moscow. Putin countered with the conquest of Crimea, making clear that these popular movements now faced the prospect of Russian intervention, including ground forces.

Continuing to pressure Ukraine, Russia at first repeated the Crimean pattern of supporting internal forces willing to engage in violence to challenge Ukrainian rule. In the Donbas in eastern Ukraine, a region home to a large Russian population, Putin supplied arms to dissidents and at times committed Russian paramilitary forces foisting a battle onto the again reluctant Ukrainian government. As this struggle continued over an extended period of time, Russia appeared unwilling to seek annexation and instead hoped that that state could come under the umbrella of Russian influence, if not in declarations of subservience then in the unsettled

[48]. Mary Ellen Connell and Ryan Evans, "Russia's 'Ambiguous Warfare' and Implications for the US Marine Corps," CNA (May 2015): 9.

notion of state security.[49] To this end, Russia turned to a sophisticated cyber effort and one tangibly more physical than seeking an information operation success by inciting internal dissent. Instead, Russian cyber attacks successfully targeted the Ukrainian power grid in December 2015. That act forced three distribution centers offline for several hours impacting 220,000 residents.[50] This strike represented strategic cyber power, but Russian forces unleashed tactical actions as well. Malware helped Russian-backed rebels in the Donbas attain the "locational data" of Ukrainian artillery and target those units for destruction.[51] Altogether, the concept that Russia sought to test cyber capabilities in conjunction with acts of war gained much credence. In the seams between cyberspace and ground conflict came an effort to enable a physical means of disruption on the ground which coexisted alongside the same effort of physical disruption via cyberspace. That challenge indeed left its victims in the grip of a seemingly perpetual assault that reminded nations to think twice about embracing connectivity as a means of feeding a global democratic inevitability.

STRATEGIC ASCENDANCY: Russia on the Attack

In Russian hands, a deliberate effort to curb any notion of a shared online space hosting a community of users to achieve a more enriched body politic came by conducting cyber attacks alongside deploying paramilitary force in neighboring countries. But a longer reach was needed to impact world events where the confrontation would be strictly cognitive. One could not

---

[49]. Mark Galeotti, "Hybrid, Ambiguous, and Non-linear? How New is Russia's 'New Way of War'?" *Small Wars and Insurgencies,* Vol. 27, No. 2 (2016): 285.
[50]. Michael Connell and Sarah Vogler, "Russia's Approach to Cyber Warfare," CNA (March 2017): 20.
[51]. "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," Crowdstrike Global Intelligence Team, December 22, 2016; then UPDATED (corrected): "Use of Fancy Bear Android Malware in Tracking of Ukrainian Field Artillery Units," Crowdstrike Global Intelligence Team, December 22, 2016. March 23, 2017. https://www.crowdstrike.com/resources/reports/idc-vendor-profile-crowdstrike-2/

simply stand by and receive the daily offensive from those enjoying connectivity in cyberspace. Blunting cyber activities to secure internal and even regional consolidation was one priority, and turning openness on its head the other. It would not be a big leap to use cyber to sow doubt in an adversary's national sovereignty well beyond Russian borders. The primary target was obvious. The online threat had to be met at its source, and that meant eroding the standing of the creator of this platform, the United States.

It did not take much to cast American confidence in the democratic process in stark relief to a technological age that exposed that very sentiment as obsolete. Unleashing an army of trolls dispensing fake news has almost done the trick of getting the United States to distrust and question an open internet. To distribute disinformation was not new. To sow doubt in trusted institutions was not new. To inject paranoia into the American body politic was not new. What was new was the willingness of that public to accept these efforts as proof of untrustworthy online interaction, of seeing only a nemesis in cyberspace. Openness became the foremost casualty of now suspicious interactions in cyberspace, as had to be the case from Russia's point of view, to offset the strategic ascendancy inherent in that very act of being online. Exchanging and sharing information among internet users became more a worry, less a right.

This success meant a Russian strategic high ground in cyberspace and this was no small accomplishment given the threat the platform had posed to an authoritarian Russian state. The nemesis of cyber rebellions at present appears quiescent. Putin again stood for election in 2017 and according to media reports won an overwhelming mandate. That success points to very little political opposition or unrest within Russia, suggesting the potential for online activism appears well under control. Moreover, the hack of the US presidential election indicates that Putin has learned his lessons well and authored his own form of cyber rebellion within US borders

designed to undermine democracy.[52] The response in the United States to better defend cyberspace means a retrenchment from openness and a further gain for the Russian strongman. In seeking greater online security, Americans no longer press the advantage of an open internet giving a voice to political expression. In abandoning the ideological high ground in cyberspace, US officials offer Russia a much sought-after reprieve from facing political rancor and agitation in a nation that otherwise does not allow such dissent. That discourse is, of course, the hallmark of democracy, not a call for oversight as Putin would have the world believe. It seems too many Western leaders must relearn this basic lesson in representative government and protect the right to information and what amounts to virtual assembly online. The United States must serve as a measuring stick for the rest of the world and then reap a concomitant benefit from the ideological dimensions of cyberspace. In that scenario, Russia would again be forced to play defense.

States endorsing political plurality merely have to defend and advance openness to blunt the Russian cognitive offensive in cyberspace. As was the case during the Cold War, an ideological struggle between authoritarianism and liberalism has again become central to US-Russian relations.[53] When Cold War parameters help shape cyberspace, a new period of containment emerges as a means of defending openness in that domain. This cognitive stand online cements ideology as paramount in conflict by ensuring an arena of shared values that challenges authoritarian rule, a success that would mean the strategic initiative lays in Western hands or all those favoring openness. Better still, openness is already US policy, is already endorsed by the private sector that does so much to shape that domain, and is already a means of delivering a nonviolent offensive in a war no less imperative to win than a physical war in other

52. Connell and Vogler, "Russia's Approach to Cyber Warfare," 24.
53. Michael McFaul, *From Cold War to Hot Peace: An American Ambassador in Putin's Russia* (New York: Houghton Mifflin Harcourt, 2018), x-xi.

domains. This recognition means US efforts must not await a ground war to team with cyber capabilities and thereby present a familiar picture of war. Rather, one must embrace the ideological struggle online and currently ongoing to maintain the permanent strategic advantage of openness in cyberspace. From that strategic high ground, one can go on the attack in cyberspace by offering a universal appeal to an online global commons that serves democracy.