Feed the Bears, Starve the Trolls:

Demystifying Russia's Cybered Information Confrontation Strategy

Nina A. Kollars, Ph.D.
United States Naval War College
Strategic and Operational Research Department
Newport, RI, USA

Michael B. Petersen, Ph.D.
United States Naval War College
Strategic and Operational Research Department
Newport, RI, US

***Abstract*— This paper seeks to establish an explicit connection between Russian strategic information operations theory and the execution of Russian cyber operations. These operations are part of a larger strategic construct in the Russian lexicon known as "Information Confrontation,"--a concept that is deeply embedded in Russian strategic thought and official doctrine. Furthermore, within the information confrontation concept, the Russians posit an essential distinction--technical and psychological effects. Using this distinction, we attempt to introduce analytical clarity to the study of Russian activities in the cyber domain. Specifically, within the technical/psychological distinction, we find that Russian operations that tend toward the latter tend to be less sophisticated and conducted at some level of remove from direct control by the regime, while the former clearly demonstrates, what we refer to as 'organizational sophistication.'**

Keywords— hacking, organizational structure, Russian strategy, cyber, APT, information operations, Russia, resources, doctrine

I. Introduction:

The flood of fevered reports on Russia's elections meddling, malware assaults, and mysterious hacking teams is fundamentally disorienting. It can make stepping back to assess Russian strategic lines of effort, and the "who" and "what" of their assets in play, seem like a fool's errand. But there is a well-established strategic and organizational logic that underlies all of these activities. What might be called "cybered information confrontation" is at the center of a Russian strategic concept known as "New Type Warfare," an intellectual construct embraced by Russia's military leadership that posits in part that the exploitation of information offers Russia a key asymmetric advantage.

II. Russian Strategy and Cybered Information Confrontation

Russian political and military leadership believes that their country is locked in an existential contest with the West. However, to the Russian mind, the very rules of this struggle have changed. The essential separation between peacetime and wartime no longer exists, and while the threat of military force is still an important component of strategy, it has receded in favor of non-military measures. Instead, global competition with the West has become a contest between who can best exploit the non-military aspects of conflict to the greatest strategic gain. In the words of General Valery Gerasimov, the Chief of Russian General Staff, "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."[1] Foremost in Russian strategy among these non-military aspects of conflict is the notion of "Information Confrontation" [*informatsionnoye protivoborstvo*].[1]

While this concept can encompass open propaganda, state-sanctioned news outlets, and other activities, cybered information confrontation is the critical component of Russia's competitive efforts. It nests within Russian strategic and military thinking as both concept and enabler. It also operates in peacetime and wartime, and its tactics range from now widely-known information operations to sophisticated hunts for and exploitation of network vulnerabilities, up to and including achieving kinetic effects in the real world. While more work remains to be done, from a command and control perspective, there appears to be a spectrum along which these functions operate, from minimal state control to extraordinarily sophisticated operations requiring strict state organization and orchestration. Along this spectrum, and in most cases, Moscow is able to achieve what it views as a level of plausible deniability by either exploiting proxies or by embedding its operations in the deeply secret world of intelligence operations.

Weaponizing information is a key aspect of Russia's competitive strategy. Indeed, information confrontation is the red thread running through every arena of strategic competition with the West. It is a strategy that seeks to exploit information in political, cultural, social, economic, religious, military, and other spheres. Information can be exploited for tactical and strategic gain, destroyed, planted, distorted, stolen, and manipulated. These techniques of course have historical precedent in the Soviet Union and the Cold War, but current

The views and opinions expressed in this article are those of the authors and do not necessarily represent the view of the Navy War College, Department of the Navy, or the Department of the Defense.

[1] There is a rich debate in Russian sources over the terms "informatsionnoye protivoborstvo" (информационное противоборство -- information confrontation), and "informatsionnaya voyna" (информационная война -- information war). In practical terms, these are distinctions without a difference, given how Russia operationalizes the concepts.

measures go beyond Soviet traditions in that they exceed mere psychological operations, and information dominance has replaced military mass in the minds of Russian strategists and policy makers as the center of gravity in a modern conflict.

Cybered information confrontation can take many paths to many goals. In some cases, the goal is merely to inject doubt in the institutions of an adversary state, to paralyze decision making, and/or to debilitate democratic processes.[2] This may either be an end in itself,or may also be part of a broader enabling campaign to achieve more specific strategic gains. In other cases, they can seek out and exploit weaknesses in network and physical infrastructure, again, either as an end in itself or to enable wider operations.

These ideas are fundamental to Russian military and political strategy. For example, Colonel V.N. Gorbunov and Lieutenant General S.A. Bogdanov, two of Russia's most influential military strategists, write that "Weakening a country marked as a target of aggression today (and also in the long run) is possible by internal weakening of the state in all respects, including the taking of informational, psychological, moral, climatic, and organizational measures…"[3] Undermining an adversary state's ability to govern, either in peacetime or wartime, is therefore both an end and an enabling tool.

This notion received its fullest expression in a 2015 article in the Russian Bulletin of the Academy of Military Science by then chief of the Main Operations Directorate of the Russian General Staff General-Lieutenant Andrey Kartapolov. Kartapolov outlined the concept of "New Type Warfare," which encompasses political methods to bring about changes in the policies of other states, political efforts to prepare the battlefield for military action, and, if necessary, high-technology conflict. The ultimate goal of New Type Warfare is to reduce the adversary's military strengths via other means. "Nonstandard forms and methods that will make it possible to level the enemy's technological superiority are being developed for the employment of our Armed Forces," he wrote. In this case, "nonstandard forms and methods" include cybered information confrontation as a tool for achieving a broader end.[4]

Intrinsic to New Type Warfare is the concept of the Initial Period of War (IPW). Information superiority, that is, controlling the flow and content of information, is the essential element of the Initial Period of War. The key, according to Russian strategists A.V. Serzhantov and A.P. Martoflyak, is "information warfare measures undertaken in advance to achieve political aims without resort to armed force, and then to cultivate a favorable response from the world community to the use of armed force."[5] Information confrontation in IPW is used to reduce public faith in national institutions and make target nations ungovernable by undermining its leadership and key infrastructures. Ultimately, for Kartapolov, "…The employment of independent actions and methods for a new type war makes it possible to achieve military results … without the employment of one's own armed forces." Thus, in this formulation, cybered information confrontation is both an end and a means of achieving strategic success.

It should be noted, however, that these ideas are also partially the result of Russia's conventional military and economic inferiority with the West, and of its search for asymmetric solutions to this challenge. This basic idea of finding cheap asymmetries against adversaries is deeply embedded in the highest levels of the Russian military and political hierarchy. No less a figure than Vladimir Putin himself has stated that "We must take into account the plans and directions of development of the armed forces of other countries… Our responses must be based on intellectual superiority, they will be asymmetric, and less expensive."[6] Likewise, in his seminal article on New Type Warfare, Kartapolov noted that "…The features of preparation and conduct of new-type warfare are being fully used, and 'asymmetric' means of confronting the enemy are being developed." Cybered information confrontation is therefore a tactic designed to short-circuit the West's military superiority by avoiding expensive and bloody kinetic conflicts, as well as achieving strategic gains by exploiting the information domain. In case a conflict were to erupt, the use of cybered information confrontation can help exploit vulnerabilities and level the playing field.

Broadly speaking, cybered information confrontation has two components in the Russian formulation: "informational-technical" and "informational-psychological." Information-technical measures tend to involve computer network operations, such as attack, defense, espionage, and exploitation.[7] Information-psychological measures are attempts to either change people's beliefs in favor of Russian strategic objectives, or to sow dissent among adversary nations to the point that decision making is hamstrung. Moscow employs these measures in both peacetime and wartime.

The most basic and well-known of these two approaches is the information-psychological approach. At the most simplistic level, Russian agencies utilize ostensibly private armies of trolls to manipulate with a certain level of plausible deniability the narrative of particular stories in an adversary country. The most infamous of these is of course the Internet Research Agency, which flooded the United States with fake news stories during the 2016 presidential election. Official Moscow attempted to maintain a degree of separation from this operation by using its connection to Yevgeny Prigozhin, the St. Petersburg restaurateur-cum-oligarch known as "Putin's Chef," who bankrolled the IRA with a portion of the billions of dollars paid to him through a foodservice contract with the Russian military.

Russia also exploits the work of semi-autonomous patriotic hackers and hacker organizations such as CyberBerkut. This

loose network of hacktivists, named after Berkut, the now disbanded Ukrainian police force that became well-known for its violent tactics against Euromaidan protesters in 2014, is, according to the Defense Intelligence Agency, a front organization for state-sponsored cyber activities in Ukraine.[8] CyberBerkut generally focuses its efforts on low-level harassment and propaganda campaigns such as DDOS attacks, website defacement, and disinformation campaigns, but has more recently been involved in email hacking schemes.[9]

Campaigns like those conducted by the IRA and CyberBerkut are possible because the distinctions between state and private in Russia have blurred almost to the point of irrelevance. Particularly under Putin, institutional boundaries have become porous, allowing private citizens and organizations to conduct sanctioned state activities, and allowing the state to mine society for autonomous assets to carry out state functions. This is part of a broader trend of deinstitutionalization in Russia, in which the boundaries between private and state, civilian and military, legal and illegal, and state and private, are quickly disappearing, if they ever existed at all. In Russia this encourages a blending of these institutions in an effort to achieve strategic gains.[10]

Information-Technical operations tend to be aimed at more specific targets and involve more malicious intent than simple psychological operations. Depending on the sophistication and the strategic aims of a given operation, the organizations carrying out these activities may be associated with or directly a part of Russian intelligence organizations. The intrusions on the DNC servers perpetrated by Cozy Bear and Fancy Bear, which are affiliated with the SVR and GRU, respectively, are only the most well-known and least sophisticated examples of information-technical operations. Much more sophisticated and worrisome is the malware Ouroboros, which, when installed on a network, gives its developers full and covert access to all of the files on that network; and Crash Override, which Wired magazine called “the most evolved specimen of grid-sabotaging malware ever observed in the wild.”11] Given their complexity and sophistication, both are widely believed to be products of Russian intelligence services.

Operations within the psychological and the technical domains exist along a spectrum. On one end are the straightforward information-psychological operations designed to influence opinion. On the other are the malicious information-technical operations that are capable of real-world effects. In between lie operations ranging from covert observation, exfiltration of information, and network control. To be sure, these operations can overlap and influence each other. For example, data exfiltrated in the course of an espionage campaign that uses advanced persistence techniques can, and likely will, be leveraged as part of a psychological operation over time.

III. Organizational Sophistication

Russia’s overall domestic hack-capacity is relatively high given its emphasis on applied mathematics and computing well-prior to college. This, combined with a proliferation of online tools that enable simple attacks like DDOS and website defacement, provide ample opportunity, low resource requirements, and highly permissive environments through which low-end, unsophisticated ‘flash mob’ style disruption can be conducted. This foundational resource base of potential hack types is part of why Tim Mauer refers to Russia as a country that ‘sanctions’ its proxy hack community in regional engagements in Estonia, Georgia, and Ukraine.[12] Simultaneously, Russia develops new malware and regularly conducts cybered operations on physical infrastructures, and conducts industrial espionage campaigns. So how can we meaningfully analyze this elusive and illusive set of agents and behaviors? And what can it tell us about their strategic priorities, risk acceptance, and approaches to cyber operations? From the perspective of defense, cyber attacks may all appear to blend together. But there are distinct stability and resource costs that separate the technical and the psychological.

While we may not be able to actually identify and count Russia’s hack army, and while we cannot know, with certainty, what zero-day and malicious software will appear in their arsenal, we can think about resources, skills, and platforms. That is, we can ask what organizational support structures are required to maintain particular lines of effort. Advanced malware development like Ouroborus and Crash Override need time, space, and resources for development. To deploy the malware, an operation needs effective intelligence, higher level coordination with commander's intent, and political top cover. Assuming that there are dedicated anti-hacking and malware efforts, all elements of complex attacks also need consistent care and feeding in order to produce their intended effect, In this sense, sophistication matters at the organizational level beyond sheer technical savvy.

Organizational sophistication can be thought of as the overall sum of an array of resources, coordination, procedures, and practices.[13] Highly sophisticated organizations provide individuals with an internal environment that supports consistently clear patterns of function. Those patterns may be tacit or explicit, but they are stable. In particular we would expect to see a high degree of sophistication in environments where teamwork across different roles is a regular occurrence (both internally but also potentially externally).

In articulating this notion of sophistication, we want to be careful to say that we are not attempting to establish any necessary relationship between success, efficiency, or even effectiveness and organizational sophistication. Nor is it the case that a high degree of internal organizational sophistication necessarily means that the organization can coordinate well with other entities. Rather, what we are pointing to is that some kinds of cyber operations/information operations appear to require more or less organizational sophistication than others. In the Russian case, the organizational sophistication demonstrated appears to break roughly along the range of the psychological and the technical aspects of the Russian strategic approach.

A. Information-Psychological

The capacity to conduct broad-based information operations does not--in and of itself--demonstrate an expansion of an adversary's capabilities. Despite continued journalistic hand-wringing regarding Russian social media and information meddling campaigns,[14] the organizational resources necessary to sustain behaviors like those exhibited by the IRA, let alone CyberBerkut, are decidedly shallow. That is, the necessary skill and sophistication level of these entities needn't be particularly high to make these groups disruptive. To even refer to their social media activities as 'hacking' is an abuse of the term. Using false messages to disrupt publics isn't even social engineering (hacking the human rather than the machine to bypass security).[15] In short, as any two-year-old can demonstrate, it doesn't take much skill or sophistication to break things.

However, this lack of sophistication may also result in high resiliency against efforts to stop or defeat them. As a question of skill and resources, media disinformation is not a complex endeavor in the contemporary era. Faux content, and the relatively mindless work of creating fake accounts to generate clicks is labor that requires, at best, some degree of ability in the target country's language and a terminal connected to the internet. Thus, disinformation production organizations, as a state sponsored service, have no necessary need to establish long-term internal stabilization structures.

From what we know of the IRA's fly-by-night structure, the work was seasonal at best, using ad-hoc hiring practices and a willingness to corral and pay the labor.[16] For this, a regime can easily outsource the work--as it did with Yevgeny Prigozhin, the Kremlin-linked oligarch and former hot-dog salesman in St. Petersburg.[17] As we have already noted, Prigozhin bankrolled the IRA by using a portion of the billions of dollars provided by the Russian government for food service for the military. The stability of such funding can ebb and flow as strategic need dictates. With low technical barriers to entry, the labor pool is deep, and personnel need little training or support. In the Russian case, this simply amounts to an ability to write, click or elevate noxious messages on already user-friendly platforms like Twitter and Facebook.

Similarly, 'patriotic hackers' with high prestige levels, like CyberBerkut, wade in markedly unsophisticated waters, both technologically as well as organizationally. Generally, groups like these are the most loosely affiliated with state efforts. Patriotic/hacktivist agents whose capabilities require little to no coordination beyond what Tim Mauer defines as sanctioning--the permission to operate against a regime's adversaries.[18] Certainly, the group has garnered global notoriety for successfully blocking public access to a few German government websites in 2015 and its more recent blog post "leak" of unverified documents linking Ukrainian political leaders and laundered funds to Hillary Clinton's 2016 campaign.[19] Nevertheless, TrendMicro's analysis of the group's membership and internal squabbling dynamics provides unexpected levity.

According to data previously available on Pastebin in 2015, the menace known as CyberBerkut has at least four active members ranging in age from 24 to 38 years. The group's most active member is 'Mink,' who also goes by the name Zac Olden. Mink previously set up a fake website intended to mimic a legitimate online store that sells Australian (specifically Tasmanian) jewelry beads.[20] Mink was also the leader of 'retribution network' whose site as well as the previous fake site have lagged or gone offline entirely. The group's instability becomes clear in 2014 when a fallout between Mink and two of its other members led Mink to doxx his own colleagues MDV and artemova in Pastebin posts. And only later in October of 2014, after the apparent doxxing, a second CyberBerkut twitter account @cyberberkut2 was created.

The misalignment and frequent interruptions of the group's activities, coupled with their relatively weak technical capacity, reveal a high prestige group with no reliable resources, stability, or real infrastructure. Its stop/start net presence and hacking behavior suggest a tiny membership footprint with limited support. If CyberBerkut could be called an organization, it is one with a nearly immeasurably small level of sophistication. While we do not doubt that there may be pro-Russian hacking groups with greater degrees of organizational complexity, this one serves as a reminder of the limitations and ephemeral nature of the volunteer group dynamic.

We should note here that while the proxy work of the Internet Research Agency and CyberBerkut offer the Russian government a certain level of deniability, the risk in exploiting these actors is that the more deniable they are, the less control the government has over their activities. This may result in unsanctioned operations that are carried out for narrow, parochial reasons instead of national strategic gain, but that may nevertheless be destabilizing. Further, the fractious nature of an organization like CyberBerkut makes it an unreliable proxy for the government. Because Moscow emphasizes deniability over control in these operations, the likelihood of these actors conducting operations that aggravate their tacit supporters is higher than if they were under strict government oversight.

Overall, it appears that Moscow has assessed a relatively low risk of reprisal to information-psychological measures and low-level technological operations like DDOS attacks. Reliance on cheap, unsophisticated proxies such as the Internet Research Agency and CyberBerkut carries, despite the state's tenuous control, almost no risk. Sanctions imposed on individuals like Prigozhin, (whose reaction was a shrug and a "Now I'll stop going to McDonald's,") and the declaration of a few Russian intelligence officers in the U.S. as persona non grata (and whose positions may by now have already been

backfilled) impose almost no cost. There is almost no serious consequence in response to these activities, demonstrating that there is likewise almost no strategic risk taken on by Moscow in its use of proxies to conduct information-psychological measures.[21]

B. Information-Technical

In contrast to the organizational simplicity of Russian information psychological operations, the Russian approach to technical operations shows evidence of a much deeper bench of cyber agents that demonstrate team-based technical collaboration in design, execution, and support. In other words, there is likely a highly sophisticated organization (or a number of them) in the background--a system with consistent resources, stability of platform, and continuity of personnel with role-specific skill sets. Both Fancy Bear and Cozy Bear hacking teams are obviously two well-known examples of long-term malicious agents that conduct technically sophisticated attacks globally. But more importantly, any APT (Advanced Persistent Threat) group is a likely suspect for high organizational sophistication given its emphasis on long-term operations and continued curation of new potential targets. Of the APT attacks attributed to Russia, it may not be as important to discern which Russian hacking team is responsible for a particular attack,[22] so much as asking whether the attacks themselves demonstrate the existence of a sophisticated organization underneath.

To wit, the 2014 appearance of the espionage toolkit named Ouroboros (Turla, Snake) and the subsequent appearance of the industrial control system malware Crash Override (Industroyer) in 2016 are two of the most advanced pieces of malware to have emerged in recent years. Both cases suggest long-term planning, support, and dedicated development of breach and exploit processes.

Russian meddling in secure government systems, and critical infrastructure attacks through the development of sophisticated malware is a consistent component of the Russian technical approach. Ouroboros' evolutionary roots date well-prior to its February 2014 christening during media coverage of the Ukraine attack during the ouster of Viktor Yanukovych.[23] Ouroboros stands as one of the longest-running continuously evolving malware platforms of its kind. As early as 2006, security research firms have obtained malware samples known generically as Agent.BTZ. Agent.BTZ has been found on U.S. government military systems, as well as other military systems globally. Privately, as firms individually have dissected and traced the malware, they began to give the generic label their own names, including Snake, Sengoku, and Snark.[24] Its meagre roots evolved over time into a highly sophisticated attack system that continues to plague government and industry alike. Ephemeral and less professional groups are unlikely to maintain this level of fortitude in sustaining the evolution of this malware.

In 2016, Crash Override infrastructure attacks on Ukrainian electrical grids were not in themselves particularly noteworthy. After all, the Ukrainians have been suffering electrical grid attacks leveraged by Russian attackers since 2015, and the Ukrainian electrical grid is supported by a series of analog backups, so damage was more limited.[25] What was noteworthy about Crash Override was that the attack platform was modular. That is, the malware was specifically constructed so that it could be adapted to other systems, not simply Ukrainian electrical systems.[26] Orchestrating an attack on a power grid needn't require any particular level of organizational sophistication. Designing malware that can be adapted to future conditions and attacks speaks to long term planning, persistence, and flexibility at a minimum, and the opportunity to experiment with the tools elsewhere and in other contexts.[27]

Another potential indicator of sophistication that is specific to cyber operations is the emergence of 'false flag' operations--the emulation of tactics, techniques, and procedures (TTPs) of another malign actor in order to pin an attack on them. The 'Olympic Destroyer' attack that disabled critical Olympics IT systems and left behind a forensic signature that mimicked that of the North Korean hacking team Lazarus Group.[28] It is one thing to copy code, but another entirely to know another agent so well that you attempt to mimic their TTPs. It also suggests that the attackers actively analyze the behaviors of other threat actors operating in this domain. Though attribution to a specific Russian ATP is under debate, political analysts argue that the timing of the false flag attack strongly aligns with Russian sentiments.[29] Security experts at Kaspersky also indicate that whomever perpetrated the Olympic Destroyer attack held their capacity in reserve--thereby suggesting that the group may be withholding its capacity for another attack in the future.[30] Both the false flag operations and holding capacity in reserve suggest an organization that intends to persist and continue operations into the future.

Available evidence is scant, but it appears that Russian political leadership may believe that these more advanced technical operations carry much greater strategic risk. If this is true, tighter state control of a more sophisticated organization than CyberBerkut, for example, would be merited. Grid hacking malware could result in the deaths of foreign citizens, especially the more vulnerable aged and infirm. Operating covert malware designed to exfiltrate information or take over systems requires professional espionage tradecraft measures. If these cybered espionage measures were directly attributed to Russia, or if the Russian government were to lose control of these capabilities, the blowback is potentially enormous. Operating such sophisticated programs may force a reliance on more professional, and professionalized, organizations such as the GRU's Fancy Bear and the SVR's Cozy Bear. Embedding these programs deeply in Russia's intelligence establishment therefore allows for better risk management and more reliable, consistent, and evolving operations, while still maintaining a level of deniability.

All of these agents, attacks, and malware demonstrate clear evidence of high levels of organizational sophistication. They require strategic leadership, political cover, consistent funding, stable platforms, skilled technicians, and the kinds of resources that point to concerted, clear efforts by Russian organizations to move competition in the cyber domain forward beyond its far more simplistic information-psych cousins.

IV. Implications and Future Research

How can organizational sophistication analyses matter to U.S. national security policy—particularly in a time when the leading stories of the year are almost entirely about cheap low-cost disruptive information operations? Thinking about organizational sophistication redirects our thinking away from the 'weapon' and toward a state's intentional development and maturation of capabilities. To be clear, while information operations can and likely do have effects, the Russian case demonstrates where stability, control, and funding are prioritized. The intentional development of a highly skilled set of hacking crews who can both breach and exploit U.S. systems is consistent with behaviors we would expect to be deployed, in both peacetime and wartime efforts. This distinction may matter when a nation is working through responses to cybered operations. Namely, which aspects of Russian-supported operations the United States should consider as an offensive action that necessitates offensive counters, and those operations that fall below such triggers and necessitate domestic resilience-building measures. In brief, it may help draw clearer conclusions to who should respond, and how.

While it may not be the case that organizational sophistication necessarily breaks along the psychological/technical divide. The case here is that it does. The damage wrought by technical attacks that produce physical effects or result in the loss of national security secrets are effects for which the military and the intelligence community are traditionally tasked—but they cannot do so for all attackers. Conversely, it remains unclear just exactly how or why a bot campaign run prior to an election necessitates a response via offensive operations. However, the sophistication of organization demonstrates some degree of measurable and documentable political intent. Particularly, the longer timelines of operation with similar patterns of behavior in a coordinated cyber campaign, make it justifiable to conduct counter and even offensive operations.

Conversely, those operations that lack organizational sophistication, also demonstrate lower capacity for traceable direct mechanisms, lower commitment to sustained effort, and less direct control by a regime. Under such conditions, the response should perhaps turn inward rather than offensive. That is, in the absence of clear long-term organizational development by an adversary, the mechanism for security may be increased domestic regulation of social media platforms; creating more resilient communications networks; and investing resources in civilian cyber education and hygiene. This is not to say that such information operations do not pose a fundamental threat to the nation, and its democratic processes. If the proposed mechanisms and their effects in disrupting democracy are found to be effective, it definitely does. But the degree to which this is a concern for foreign operations by military and the intelligence community must be much more aggressively clear than is the case currently.

The genuine concern, in the eyes of the authors, in the case of Russia, should be toward the technical. Not simply because the technological sophistication levels are high--but because the organizational requirements to maintain the style and methods demonstrated in the most recent Russian attacks on Ukrainian infrastructure suggest tight coordination and planning that only a sophisticated organization can provide. Specifically, there is sufficient evidence both in the orchestration of attacks as well as in the platforms and resources utilized to necessitate stable, consistent organizational structures that endure over time. That is, the discernment of the "distance from, or the nature of the relationship to" the state may be more important in understanding the strategic goals and possible persistence of these activities, than direct identification of who is employed by, sponsored by, or even permissively permitted to act as part of the approach.

Furthermore, less sophisticated information-psychological operations may be more resilient, and more resistant to measures designed to defeat them. Information-psychological efforts draw on a massive labor pool and an informal network, so efforts to defeat them at the source are mere games of whack-a-mole, and efforts to defeat them at home run the risk of becoming dangerously undemocratic. This being the case, the investment in researching and countering these operations particularly in terms of thinking offensively, may not be worth it. Government and social media corporations can and should be vigilant, calling out and removing disinformation efforts, but disinformation and low-level harassment campaigns are ultimately almost impossible to eliminate. The only other option may be in developing means to spread truthful information and news to local populations in Russia. The United States has apparently made a policy decision to avoid this, despite the fact that it does so in places like Iran, North Korea, and elsewhere.[31] Finally, the capacity to conduct information disruption through online social media campaigns is poised to become an even more crowded space since the cost is so low. We have already seen numerous efforts, not simply by states, but by rebel groups and terrorist organizations to drive and influence via these platforms. If we haven't already witnessed it, we will increasingly see the rise of the rest—of small states and non-state actors making these platforms even more noisy.[32]

In summary, it is the opinion of the authors that research energy can and should focus on understanding the strategic goals, structure, resources, and ideas that specifically address Russian information-technical operations. It is our opinion that the psychological component is not only more difficult to control as a function of offensive or non-domestic efforts, but that there is not anything particularly unique about the ability to influence populations through social media. Thus, the psychological efforts are likely to be leveraged by weak and strong adversaries both symmetrically and asymmetrically.[33] The general noisiness of such low-end efforts makes understanding the unique lines of Russian effort more difficult to discern. In contrast, following the resource and stability needs of mature efforts of the technical side will likely yield more meaningful specific insights as pertains to Russia-specific concerns.

This is not to suggest that U.S. agencies should match or mirror Russian efforts per se. But a clear-eyed assessment of where and just how much resourcing is being directed by an aggressive adversary can help shape our own policies

regarding where and how our strategic trade-offs are positioned. Specifically, the current paralysis exhibited in DoD counters to Russian cybered moves, is partially about which moves should be understood heartburn and which as heart attack. We have posited here that more clarity between these actions should rest on the sophistication of the organization that underlies the action, rather than the activity itself. In this way, the United States and its partners will be able to develop and ensure that standards are met for hardening critical infrastructure against cyber intrusions and attacks with an eye toward risk management rather than seeking unattainable 100% security goals. To be certain, much of this effort is currently left to the private sector to manage. But In addition, a better understanding of the organization structure behind malicious technical operations, their purpose, their motivation, and their intended effect, allows us to develop deterrence measures as well as timely and appropriate responses in those cases that can be attributed.

REFERENCES

[1] Valery Gerasimov, "Znachie nauki v prognozirovanii," ["The value of science in prediction"], Voenno-promyshlennyi kur'er [Military-Industrial Courier], Feb. 27, 2013.V.N. Gorbunov and S.A. Bogdanov, "Armed confrontation in the 21st century," Military Thought, 1 (2009), 21-22. Emphasis in original.I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[2] Paul, Christopher, and Miriam Matthews. "The Russian "Firehose of Falsehood" Propaganda Model." RAND Corporation (2016). Accessed September, 17, 2018. https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf

[3] A.V. Kartapolov, "Uroki voennyh konfliktov, perspektivy razvitija sredstv i sposobov ih vedenija. Prjamye i neprjamye dejstvija v sovremennyh mezhdunarodnyh konfliktah," ["Lessons of military conflicts, prospects for the development of means and methods for delivering them, direct and indirect actions in contemporary conflicts,"], Vestnik Akademii Voennyh Nauk [Bulletin of the Academy of Military Science] 9 (2015), 2. See also Timothy Thomas, "The Evolution of Russian Military Thought: Integrating Hybrid, New Generation, and New Type Thinking," Journal of Slavic Military Studies, Vol. 29, No. 4 (2016).R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[4] A.V. Serzhantov and A.P Martoflyak, "Modern military conflicts," Military Thought, 2 (2009), 88.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[5] Vladimir Putin, "'Soldat est' zvanie vysokoe i pochetnoe' [The rank of 'soldier' is honorable and respected], Excerpts from the Annual Address to the Federal Assembly of the Russian Federation," Krasnaya Zvezda [Red Star], May 11, 2006.

[6] Defense Intelligence Agency, Russia Military Power: Building a Military to Support Great Power Aspirations (Washington, DC: Defense Intelligence Agency, 2017).

[7] Timothy, L. T. "The Russian Understanding of Information Operations and Information Warfare." The Information Age Military. Accessed September, 17, 0218. http://www.au.af.mil/au/awc/awcgate/ccrp/thomas.pdf

[8] Bing, Chris, "Hacker group 'CyberBerkut' returns to public light with allegations against Clinton," Cyberscoop,undated, https://www.cyberscoop.com/cyberberkut-returns-hillary-clinton/, accessed July 25, 2018.

[9] Mark Galeotti, Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Challenge Right (Mayak Intelligence: Prague, 2016), 48-50.

[10] G. Data Security Labs, Uroburos: Highly complex espionage software with Russian roots, https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf, accessed July 25, 2018.

[11] Maurer, Tim. Cyber Mercenaries. Cambridge University Press, 2018.

[12] There exists a robust literature in business management whose route of inquiry traces organizational structure and its outcomes on production. While there are clearly differences between the factors that produce successful corporate structures, and effective government organized/sponsored entities, the core insights align reasonably well enough to carry the concept over. See for example: Teece, David J. "Strategies for managing knowledge assets: the role of firm structure and industrial context." Long range planning 33, no. 1 (2000): 35-54.

[13] Bing, Chris. "Russian hacker group 'CyberBerkut' returns to public light with allegations against Clinton." Cyberscoop. July 12, 2017. Accessed July 25, 2018.

[14] Honan, Mat. "Social Engineering Always Wins: An Epic Hack, Revisited." Wired. June 03, 2017. Accessed July 25, 2018. https://www.wired.com/2014/01/my-epic-hack-revisited/

[15] Chen, Adrian. "What Mueller's Indictment Reveals About Russia's Internet Research Agency." The New Yorker. February 20, 2018. Accessed July 25, 2018. https://www.newyorker.com/news/news-desk/what-muellers-indictment-reveals-about-russias-internet-research-agency.

[16] "Inside the Internet Research Agency's Lie Machine." The Economist. February 22, 2018. Accessed July 25, 2018. https://www.economist.com/briefing/2018/02/22/inside-the-internet-research-agencys-lie-machine.

[17] Maurer, Tim. Cyber Mercenaries. Cambridge University Press, 2018.

[18] Bing, Chris. "Russian Hacker Group 'CyberBerkut' Returns to Public Light with Allegations against Clinton." Cyberscoop. July 12, 2017. Accessed July 25, 2018.

[19] "Hacktivist Group CyberBerkut Behind Attacks on German Official Websites - TrendLabs Security Intelligence Blog." Simply Security News, Views and Opinions from Trend Micro, Inc, 21 Jan. 2015, blog.trendmicro.com/trendlabs-security-intelligence/hacktivist-group-cyberberkut-behind-attacks-on-german-official-websites/.

[20] Reuters, "Russian businessman Prigozhin dismisses new U.S. sanctions: RIA," March 15, 2018, https://www.reuters.com/article/us-usa-russia-sanctions-prigozhin/russian-businessman-prigozhin-dismisses-new-u-s-sanctions-ria-idUSKCN1GR2G7, accessed July 27, 2018.

[21] GReAT. "OlympicDestroyer Is Here to Trick the Industry." Securelist - Kaspersky Lab's Cyberthreat Research and Reports, Kaspersky, 8 Mar. 2018, securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/.

[22] Jones, Sam. "Cyber Snake Plagues Ukraine Networks." Financial Times. March 07, 2014. Accessed July 28, 2018. https://www.ft.com/content/615c29ba-a614-11e3-8a2a-00144feab7de.

[23] "The Snake Campaign." BAE Systems | International. January 2016. Accessed July 28, 2018. https://www.baesystems.com/en/cybersecurity/feature/the-snake-campaign.

[24] Zetter, Kim. "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid." Wired. June 03, 2017. Accessed July 27, 2018.

[25] Brocklehurst, Katherine. "CRASHOVERRIDE – First Malware Platform Designed to Take Down Electric Grids." Belden. October 9, 2017. Accessed July 27, 2018. https://www.belden.com/blog/industrial-security/crashoverride-first-malware-platform-designed-to-take-down-electric-grids

[26] Greenberg, Andy. "How An Entire Nation Became Russia's Test Lab for Cyberwar." Wired. April 13, 2018. Accessed July 27, 2018. https://www.wired.com/story/russian-hackers-attack-ukraine/.

[27] Jackson Higgins, Kelly. "Olympic Destroyer's 'False Flag' Changes the Game." Dark Reading, Information Week, 8 Mar. 2018, www.darkreading.com/attacks-breaches/olympic-destroyers-false-flag-changes-the-game/d/d-id/1331222.

[28] Greenberg, Andy. "'Olympic Destroyer' Malware Hit Pyeongchang Ahead of Opening Ceremony." Wired. February 22, 2018. Accessed

July 28, 2018. https://www.wired.com/story/olympic-destroyer-malware-pyeongchang-opening-ceremony/.

[29] GReAT. “OlympicDestroyer Is Here to Trick the Industry.” Securelist - Kaspersky Lab's Cyberthreat Research and Reports, Kaspersky, 8 Mar. 2018, https://securelist.com/olympicdestroyer-is-here-to-trick-the-industry/84295/.

[30] Thomas M. Hill, “Is the U.S. Serious About Countering Russia’s Information War on Democracies?” Brookings Institution, https://www.brookings.edu/blog/order-from-chaos/2017/11/21/is-the-u-s-serious-about-countering-russias-information-war-on-democracies/, accessed July 28, 2018.

[31] Limbago, Andrea "Smaller Nation State Attacks: A Growing Cyber Menace." Threatpost | The First Stop for Security News. July 18, 2018. Accessed July 28, 2018. https://threatpost.com/smaller-nation-state-attacks-a-growing-cyber-menace/134061/.

[32] Ibid