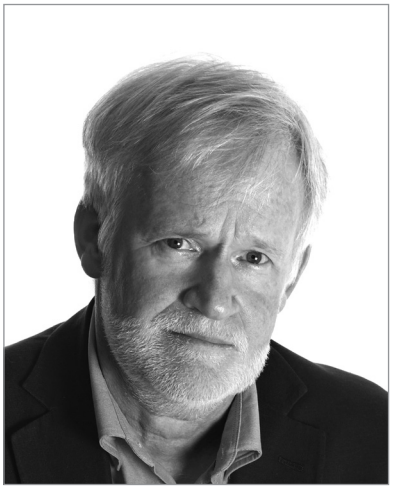
Winning Future Wars: Russian Offensive Cyber and Its Vital Importance in Moscow's Strategic Thinking

Dr. Rod Thornton
Dr. Marina Miron

ABSTRACT

This article highlights the importance of offensive cyber as an instrument for Russia to generate strategic effect against NATO and its core states. It focuses on the use of offensive cyber by the Russian military at the strategic level. This military is perceived to be the lead actor in the operationalization of offensive cyber by Moscow. Because the Russian military sees itself at an overall disadvantage vis-à-vis NATO's conventional capabilities, it is offensive cyber that it is looking to provide a means of fundamentally redressing this imbalance. Offensive cyber is a vital tool for the Russian armed forces. It is indeed viewed as being the only available instrument that can, short of the use of nuclear weapons, bring about the neutralization of core NATO states; that is, to defeat them. This neutralization can be engendered, according to Russian military logic, in two ways: either through cyber-psychological or cyber-technical attacks. This article unpacks these terms and indicates how both can theoretically generate the degree of impact that could lead to the neutralization of core NATO states. Finally, there will be a review of the Russian use of offensive cyber in the Ukraine conflict.



Dr. Rod Thornton, formerly in the British Army, teaches at the UK Defence Academy as a member of the Defence Studies Department of King's College London. A Russianist by academic background (having lived and worked in both Moscow and Kyiv), his research today focuses mainly on the Russian military, including its cyber capabilities. He has written widely on various aspects of the Russian military and teaches high-technology weapons systems at the UK Defence Academy.

INTRODUCTION

This article analyses the concept of offensive cyber when employed at the strategic level by the Russian military against core NATO states. The focus here is on understanding how important offensive cyber is to the strategic thinking of the Russian military and to Russia itself. Offensive cyber is viewed as the country's only truly war-winning tool when it comes to confrontations with actual NATO states (rather than more limited conflicts such as Ukraine).

The Russian military seeks to employ offensive cyber in two forms. The first is what is referred to in Russian as the cyber-psychological *(kiber-psikhologichkii)*. This form is being widely utilized now against NATO states in considerable depth as part of what has been described in United Kingdom government documents, and even before the Ukraine war (which is discussed below), as the "intensifying geopolitical competition" between Russia and NATO states.[1] This competition is currently characterized by restraint and conducted in the "sub-threshold"[a] space.[2]

From the Russian perspective, offensive cyber-psychological activities in this sub-threshold competition are important because they can be used to manipulate people's minds – from political figures to entire populations. The core belief in Russian military circles is that offensive cyber tools, when used as a weapon of psychological influence, can over the long term and through a process of weakening, destabilizing, and undermining from within, go so far as to defeat (or "neutralize," to borrow from the Russian military lexicon) Moscow's peer-state adversaries. This can be done without a shot being fired. Once neutralized, such adversaries, and considering Clausewitz's understanding of how wars are won,[b] can be subject to the imposition of [Russian] will, whether they are conscious of it or not.

a Sub-threshold activities are those that do not push a targeted state into a kinetic response, i.e., that do not incite armed conflict.

b For Karl von Clausewitz, the aim of war is to "compel our enemy to do our own will" (Clausewitz 1989: 75).

Dr. Marina Miron is an honorary research fellow at the Defence Studies Department, King's College London. She is also a member of the Centre for Military Ethics, King's College London. Her current research focuses on emerging and future military technologies, including drones, human augmentation, artificial intelligence, and cyber instruments, and how these impact the strategic and operational landscapes. As well as producing several publications, she has participated in numerous conferences related to cyber and information warfare and has presented on the topic at the UK MoD. Dr. Miron is currently working on a UK MoD-funded project related to the integration of human augmentation technologies in the military.

Cyberattacks in this context form a vital element in the Russian military's current strategic application against Western actors of what it refers to as its sub-threshold "active defense" *(aktivnaya oboronna)* measures. Active defense entails using predominantly non-kinetic means which are designed to fundamentally weaken NATO state adversaries and the whole Alliance structure. This notion of active defense and the important role of cyber-psychological attacks in creating the neutralization will be highlighted in this article.

The second strand of Russian offensive cyber comes in the "cyber-technical" *(kiber-tekhnicheskii)* form. This form is generally understood in the West to represent cyberattacks. These will be conducted against NATO states' information technology (IT) infrastructure and technical systems. In line with the "active defense" logic, these attacks are currently kept at a low level so that they remain definitively sub-threshold. However, if (or when?) the era of competition with NATO moves into one of very high international tension or even of actual inter-state conflict, restraint will no longer have any currency and then the genie may truly come out of the Russian military's offensive cyber-technical bottle. A series of cyberattacks that target adversary states' major IT systems can, in this scenario, coalesce to mean that such states, again undermined from within, may no longer be able to function as states. The cyber-technical attacks can, like their cyber-psychological brethren, become a truly war-winning weapon over a much shorter time frame. The shock and devastation wrought by a synergistically applied set of cyber-technical attacks can, as some Russian observers have noted, create effects akin to those of nuclear weapons.[3]

As this article emphasizes, it is essential to appreciate how much the Russian military strives to create cyber-technical attacks aimed at creating immense shock and devastation. As a cultural norm, the military sees that *all* engagements from the tactical level to the

strategic as being won most efficiently against strong opponents by striking a surprise blow of stunning, crushing power. This blow, derived from the thinking of the Soviet era, is known as the *udar.* This is noted as being a "concept rarely used in Western military thought."[4] But as Shimon Naveh expresses it, the *udar* is "one of the fundamentals of Russian military thought."[5] The shock of a well-conceived and effectively applied *udar* is one from which any adversary, be it a platoon on a battlefield or a state actor, cannot recover. The *udar* is the best way of "neutralizing" Russian adversaries.[6]

In this article, we explore why the two forms of offensive cyber—cyber-psychological and cyber-technical—hold such important places in Russian strategic thinking, both now and particularly in the near- to medium-term future. It could be the case that Russian offensive cyber may pose, in terms of strategic risk, the greatest short- to medium-term threat to both individual NATO states and the coherence of the Alliance itself. China may represent a long-term threat to the US and its allies, but Russian offensive cyber is far more the enemy at the gate.

This article engages mainly with Russian *military* writings on offensive cyber. It is perceived that this military[c] (and those associated with it, for example, the non-state hacker groups it employs)[7] is both the major player in terms of the Russian state bodies engaging in offensive cyber (through the military's intelligence arm, the GRU[d]) and also the prime mover in coordinating the activities of the state's other offensive cyber protagonists.[8] These are the internal security force, the FSB[e] and the SVR[f], the foreign intelligence service.[9] The head of the Russian military (at the time of writing), General Valerii Gerasimov, also gives the impression that it is his military that the coordinating body for the state's offensive cyber actors.[10]

Russia's strategic position as viewed from Moscow

To truly understand the vital and growing importance of offensive cyber in the Russian strategic picture, some background is required. The Russian military views offensive cyber as an essential means of providing profound strategic effect in a geopolitical environment where Moscow sees itself as being under significant threat from the West and NATO with few if any, available means of effectively countering this threat.[11]

This Western threat is said to be evidenced by a bellicose NATO (or collections of NATO countries), which has engaged in a series of post-Cold War interventions in Iraq, Bosnia, Kosovo, Afghanistan, Libya, and Syria. These stood counter to Moscow's strategic interests. Second, of course, there has been the gradual expansion of NATO to Russia's borders. Perhaps more significant, though, has been NATO's encouragement over recent years of Georgia and, more especially, Ukraine to join the Alliance. Leading Russian politicians and military figures have long been pointing out that NATO's behavior represents a direct threat to Russia and Russian

c This is also a military that has recently become Putin's most favored organ of state defense and security.

d Technically, the GRU [Glavnoe Razvedyvatel'noye Upravleniye] (Main Intelligence Directorate) is today the GU (Main Directorate of the General Staff of the Armed Forces of the Russian Federation), but the name GRU seems to have stuck.

e Federalnaya Sluzhba Bezopasnosti [Federal Security Service] operates using the APT28 group (including Cozy Bear) and others such as Turla and Palmetto Fusion.

f Sluzhba Vneshnei Razvedki [Foreign Intelligence Service] operates using the APT29 group.

interests.[12] This idea of being at a disadvantage is strongly reflected in the Russian *Military Doctrine* of 2014[13] and even more so in the *National Security Strategy* of July 2021.[14] This sense of both threats is heightened, moreover, by the acknowledgment—and made apparent in the opinions expressed by General Gerasimov and other leading figures in Russian political and military spheres—that NATO is capable of fielding armed forces that are both qualitatively and quantitively stronger than Russia.[15] The prognosis is that if any major shooting war with NATO itself does take place, then the Russian military is likely to lose heavily.[16] The follow-on from this sense of both threat and vulnerability is that Moscow's freedom of action is being constrained on the international stage. There is a feeling within Russia that the country's ability to act as a great power wielding significant influence on world events—which Moscow feels to be its rightful destiny—is being thwarted by the activities of a more powerful NATO.[17]

The actual nature of the threat

This general background threat is manifest, in Russian eyes, in two specific forms of direct jeopardy from the NATO quarter. The first comes in a kinetic form. This will be specifically exhibited, the judgment is, not so much from a nuclear attack (which is considered highly unlikely in Russian circles)[18] but rather from a surprise strike against Russia using the United States' nascent Prompt Global Strike (PGS) system (*Global'nii Udar* in Russian).[19] This consists of (according to Russian estimates) some 6,000 or so non-nuclear cruise missiles based on US surface and sub-surface vessels. Russian analysts fear these missiles could be launched *en masse* and at any time against the country's critical national infrastructure (CNI) and, literally overnight, largely destroy it. Russia could only retaliate by going nuclear, which is a decision the Kremlin does not want to contemplate.[20] However nascent it might be, a potential strike by the PGS system is still seen to represent an existential threat to the Russian state. It is noted, indeed, as being the "most serious threat facing Russia."[21]

A second existential threat that NATO is seen to pose comes in a non-kinetic form. This is the fear of a NATO-inspired color revolution that would threaten the political regime in Moscow. This is where Western soft power would be used as a weapon to weaken and destabilize Russia.[22] With the perceived Western control of the Internet and leading social media platforms, the Kremlin looks upon its population as being bombarded with favorable views of both the West and of those Russian agencies and political figures who oppose Putin and his government. These same Western sources likewise carry negative portrayals of Putin and his government. The concern is that such messaging has caused and will continue to cause domestic social unrest in Russia that may remove Putin from power.[23]

With these twin threats posed by a surprise PGS strike and a color revolution and set against a background of perceived long-term NATO bellicosity, there is a sense within Russia's civil and military hierarchy that NATO and the West more broadly, is already engaged in the form of competition that is akin to an actual (albeit non-kinetic) war with Russia. And it is a war in which Moscow feels it is at a distinct disadvantage. It has a weaker military (one getting weaker

by the day in Ukraine); it cannot match the PGS system, and it does not have the influence inherent in Western soft power. NATO thus has ways of potentially "neutralizing" Russia or of imposing its "will" on the country that Moscow cannot reciprocate with.[24]

The Russian response

The Russian response to these perceived threats appears focused on ensuring that NATO and its leading states are, above all, never in a position to take any decision to use any form of armed force against Russia. This is mostly about shaping mindsets within NATO countries. The first element here is to employ traditional deterrence. Russia has recently been beefing up its nuclear capability. The message is one that deterrence by punishment still exists in the nuclear realm.[25] Russia has also increased its territorial defense, notably through the establishment of what is known in the West as anti-access/area denial (A2/AD) bubbles around the country's borders.[26] These consist of a series of defensive weapons systems, which mostly rely on air defense and anti-missile missiles. These A2/AD arrangements are, in large part, designed to thwart the PGS system and thus generate deterrence by denial.[27]

However, while such an enhanced nuclear capability and the A2/AD defenses might deter NATO policymakers from contemplating a physical attack on Russia (which has been discussed in a 2018 U.S. Army doctrinal publication),[28] they do not offer the possibility of Russia prevailing—winning—in the ongoing non-kinetic competition/war or any future actual kinetic one with NATO forces. What Moscow feels it needs are tools that can put NATO and its core states themselves under threat.

Russian military writings ponder this situation. There is a need to find the most apposite ways to weaken and destabilize core NATO states and to undermine the Alliance's coherence so that they both are no longer able to threaten Russia physically or to stand together to stymie Russian geopolitical interests.[29] In essence, as stated by one Russian analyst, NATO must be "brought into a state where they can no longer fight."[30]

It is argued that a degree of aggression or "pre-emptive neutralization" as Gerasimov calls it, is advocated for here.[31] Still, this aggression must remain sub-threshold so as to not incite retaliatory kinetic action by NATO. Ideally, it should also be deniable so the blame for any aggressive acts should not fall on Russia.[32] The degree of sub-threshold aggressiveness currently generating this process of weakening is captured in the military's aforementioned new strategy of "active defense" [*aktivnaya oborona*].

Active defense

The necessity to specifically adopt active defense was first voiced by Gerasimov in a speech in March 2019.[33] It is a strategy that is currently being enacted by his military in the sub-threshold space in coordination with other Russian security actors. It utilizes a variety of measures, including diplomatic and economic activities and attempts to alter election results

in Western states.[34] Also included are saber-rattling troop movements. As Gerasimov states, "demonstrations of military power [will] enhance the effectiveness of non-military [active defense] means."[35]

There is an argument that these active defense measures are nothing new; merely a continuation of the traditional Soviet military's sub-threshold idea of *aktivnost´* (basically, activity) [36] and the KGB's past 'active measures.'[37] But there is something more here. Active defense today is more muscular, bellicose, and refined than its predecessors. Indeed, one renowned Russian observer of the military, Pavel Felgenhauer, has noted that Gerasimov's active defense strategy actually represents a step up in aggressiveness from what previously had been labeled as the "Gerasimov Doctrine" of 2013.[38] This was Gerasimov's original call for his military to engage in more belligerent non-kinetic actions against Western adversaries.[39] According to Felgenhauer, Gerasimov's new and even more belligerent idea of active defense should now be called "Gerasimov 2.0."[40]

One area of active defense that highlights this increased aggression is in the field of information warfare. And it is information warfare that appears, from the Russian perspective, to be the most effective element of active defense. Today, information warfare offers more than it ever did as a weapon. It offers the ability to neutralize state adversaries but with very little outlay or expense and with little fear of facing retaliatory action.[41] For a vulnerable Russian—from Moscow's perspective—and with few instruments to mitigate this vulnerability, information warfare is seen as having a truly vital *strategic* role.[42] Gerasimov has said specifically that "the study of issues of preparation and conduct of information actions is *the most important task of military scienc*e [emphasis added]."[43] Thus, it is not hypersonic missiles or artificial intelligence, or any other new technology that Russian military science should focus on, actually it is information actions.

The crucial aspect of information warfare

It is notable in Russian military literature just how much information warfare (IW) as a topic stands out. There are many discussions about using information as a weapon from the tactical level to the strategic.[44] Again, this is nothing new. The Soviet military previously placed a great deal of emphasis on the use of information as the core element of its psychological warfare activities.[45] Western militaries, of course, both in the past and very much so still today, are more wary of engaging in psychological operations, particularly at the strategic level.[46] Thus there is far more discussion within the Russian military regarding the use of IW[47] at both the operational level and, particularly, the strategic, that is simply not apparent within the militaries of Western states.[48]

This military's understanding of IW can be judged using the recent definition supplied by one of the current leading writers on Russian strategic thinking, Aleksandr Barthosh:

> A set of measures taken to achieve information superiority over the enemy by influencing his information systems, processes, computer networks, the public and the individual consciousness and subconsciousness of his population and personnel of his armed forces while protecting one's own information environment.[49]

This definition captures the general Russian view that information warfare encompasses attacks on computer networks and the consciousness and subconsciousness of civil populations and military personnel. The Russians break down IW into two mutually supporting elements: information operations and cyber operations.[50] The concept of cyber operations – or offensive cyber[g] – is then further broken down into the two distinct strands: cyber-technical and cyber-psychological.[51]

These offensive cyber operations, of course, tick all the boxes required of a Russian military active defense measure: they are sub-threshold; they are (theoretically) deniable, and they can, especially in the current era, have a considerable effect. Moreover, as noted, the Russian military sees offensive cyber as leading to the weakening and destabilizing of adversary states, and possibly to their outright defeat. Here lies the true importance of offensive cyber for Russia: it appears to offer its *only* truly war-winning weapon against NATO as a collective and against its principal state actors.[52] The Russian belief, moreover, is that such war-winning results can be achieved using either of the two strands of cyberspace operations, the cyber-psychological or the cyber-technical.

Cyber-psychological operations

Russian cyber-psychological operations at the strategic level and applied in the geopolitical environment of competition involve the use of the Internet, and especially social media platforms, to spread propaganda/black propaganda and misinformation/disinformation that can alter perceptions in targeted states across a broad political and societal range.[53] Sergei Naryshkin, the head of the Foreign Intelligence Service (the SVR) – where the SVR is a major player in Russian cyber-psychological operations[54]– expressed the general understanding as to the merits of cyber-psychological operations:

> The modern world is characterized by the fact that non-military conflicts are multiplying, and their main targets are not armed forces or military facilities, but government agencies, the political structure of societies, vital resources, and, finally, social consciousness.[55]

This form of offensive cyber, when applied over a sufficiently long timeframe, is designed to lead to a slew of outcomes positively judged by Moscow. At one end of the spectrum, cyber-psychological operations would focus on changing the decision-making calculus of leading political figures in targeted states in ways desired by Moscow. Here the aim would be to create an effect according to the long-established Soviet/Russian desire to seek strategic advantage by engaging in reflexive control measures. This is where Western politicians and military leaders would be manipulated by Russian informational inputs without their realizing it.[56] Cyber-psychological interventions can also alter the actions of governments by

g There is no specific Russian term for offensive cyber.

creating groundswells of public opinion that generate pressure on administrations. They can also involve attempts to affect election results using misinformation/disinformation.[57]

More dramatically, though, cyber-psychological operations are seen as moving beyond mere influence or manipulation to fundamentally destabilize adversary states. A chief target would be what the UK government refers to as the state's social cohesion.[58] In several countries, this can be significantly undermined by using information supplied over IT means to create or exacerbate existing cleavages within societies or to incite anti-government groups who then drive disorder. This is what Russian military doctrine refers to as making use of the "protest potential of the population."[59] This potential may be seen as perhaps the Russian military's *most potent strategic weapon* in the near-term future against NATO states.

A large body of literature in Russia is devoted to describing how to incite this protest potential or how to make a population turn against its government. This form of warfare has been variously labeled by Russian authors such as Barthosh,[60] Evgenii Messner,[61]Andrei Kokoshin[62] and Valerii Konyshev and Aleksandr Sergunin – as "mental warfare," "rebellion wars," "wars of consciousness," and "political warfare."[63]

Today there is much more fertile ground than ever before for creating social cleavages across the Western world. This is especially so given the prevalence of social media, which often drives divisive populism and general societal discord. Indeed, both the US[64] and the UK[65] have blamed Russian misinformation/disinformation for stoking unrest within their respective countries. And some inkling of the type of disruption that Russian cyber-psychological operations would hope to generate (or perhaps have generated) could be seen with the storming of the US Capitol Building on January 6, 2021.[66] Such instances can only encourage the Russian military to increase the degree, tempo, and potency of its cyber-psychological operations in the future. This is particularly so as worldwide inflation begins to bite and social discontent rises in the Western world. Of course, NATO as a collective and its cohesion is a target here. Russia appears to be generating information-driven cleavages between member states to weaken the Alliance.[67]

According to Russian military logic, states that become so concerned with their internal security are ones that then tend to lose interest in their external security. They will look inwards to threats, not outwards.[68] When applied to NATO states, the benefits to Russia are obvious. Taking any momentous decisions regarding Russia by core NATO states or the Alliance itself would be difficult to generate if they had to concentrate on domestic problems. One result might be no threat to Russia of a consensus-reliant NATO decision being made to stand up to Russian aggression on the international stage or even, with perhaps Ukraine in mind, to engage in any kinetic action against Russia itself.

And then, of course, there is also the ultimate aim of Russian offensive cyber-psychological operations. If the protest potential can be tapped into with sufficient energy and if the degree of internal *khaos* (to use a Russian word employed by some analysts) created reaches a sufficient

pitch, then this may render a state ungovernable.[69] Such a collapse of the targeted state would equate, in Russian eyes, to its neutralization, its defeat.[70]

Cyber-technical operations

In Russia's military playbook, cyber-technical operations, when used as a strategic tool against adversary states, have a different focus depending on the strategic situation.[71] In the current era of competition between NATO and Russia, they will not focus their cyber-technical activities on creating significant disruption or damage within the cyberspace and IT systems of NATO states. That is not to say that there have been no such attacks. There was, of course, the very damaging attack against Estonia in 2007, but this was related to a specific issue and was not part of some overall Russian campaign.[72] There have also been major Russian cyberattacks against (non-NATO) Ukraine in recent years that were seriously disruptive, even before the current war.[73] There have also been attacks against NATO countries that may be seen as clumsy and of no more than nuisance value in a strategic sense, including ransomware attacks.[74] There have also been attacks on electoral processes in Western countries with a cyber-technical element to them.[75]

From a strategic point of view, one can understand why current Russian cyber-technical activity would not aim to inflict major disruption within NATO states. Such acts carried out in an era of competition would serve no real strategic purpose. They would only create unnecessary diplomatic angst and might, however deniable, invite retaliation (including in the kinetic realm).[76]

Thus, while concerning to NATO states, Russian cyber-technical attacks currently cannot be seen as significant (see below regarding the Ukraine conflict). But a clear Russian game plan is apparent: such attacks can be seen largely as intrusions aimed at preparation for future activities at the strategic level. This preparation involves work in three spheres. First, cyber espionage will focus on stealing intellectual property and accessing secret information that could be useful to Russia's military and economy. The second will be reconnaissance; that is, looking for weaknesses in NATO countries' computer systems—both civil and military—that could be taken advantage of later. A third will be the clandestine planting of destructive malware in either military or CNI systems which can be triggered as part of a future "zero-day"[h] attack.[77]

The Russian aim seems obvious. Such *sub rosa* cyber-technical activities would all be designed for use during a state of actual armed hostilities with NATO or at times of high geopolitical tension when Russia no longer sees any reason for cyber warfare restraint. The hoped-for effects of a major cyber-technical assault would include:

- Turning off lights and power.
- Disabling industrial control systems.
- Crippling banking systems.
- Disrupting logistics chains (including food supplies).

h These are exploits of vulnerabilities in software not known to anyone but the hackers themselves. These exploits can be leveraged at any time (if undetected and not fixed), thereby creating a so-called "zero-day attack."

The ideal Russian outcome would be that societies could no longer function; governments would lose control, and *khaos* could be induced again. It could all be achieved within a few hours. Russia imagines that the effect of such a catastrophically damaging cyberattack would be equivalent to that of an attack by nuclear weapons.[78] Here is the cherished goal of all Russian military operations: the *udar*—the crushing, mortal blow that is delivered with speed, surprise, and force. It would be at the strategic level and generated by non-kinetic and highly cost-effective cyberattacks that could theoretically be deniable.

With this bigger prize—the *udar*—in mind and given that this concept relies for effect ultimately on surprise, it should be expected that, in the immediate future, majorly disruptive Russian cyber-technical attacks will, where NATO states are concerned, not be apparent. The attacks that occur will remain limited in scope and largely confined to the aforementioned three spheres. In preparing for an *udar,* the Russian military will not want to show its cyber hand. It values cyber shock, not cyber attrition. But it can be surmised that the preparatory work: the espionage, reconnaissance and the planting of malware will, in the coming years, only be increasing in intensity so that the eventual cyber *udar* can be made as effective as possible (see also below).

The power of offensive cyber

Of course, the two forms of cyberattack—cyber-psychological and cyber-technical—can be used together: a gradual weakening process brought about by the former can be exacerbated by a later cyber-*blitzkrieg* application of the latter. Perhaps most concerning of all, though, for NATO states is that there will be a Russian determination to integrate artificial intelligence (AI) into its offensive cyber activities in the future. AI-enhanced cyber tools underpinned by powerful machine learning will open up new possibilities in both the cyber-psychological and cyber-technical realms.[79] In the former, disinformation campaigns could become much broader in scope and more focused in their targeting due to the power of algorithms and automation. In the technical realm, AI could offer, in Russian eyes, dramatic advantages. Indeed, the combination of AI and cyber could mean, as one advisor to the Russian military believes, that the Third World War might actually be over within just "a few seconds if one state takes control of all the main [cyber] life-support systems of rival countries using AI technology."[80]

The War in Ukraine

Prior to Russia's invasion of Ukraine there was obviously much hype about the quality of the offensive cyber capabilities that the Russian military could bring to bear.[81] Ukraine and, indeed, several NATO states were prepared for a major cyber onslaught by what was considered to be the "the most aggressive cyber actor in the world."[82] But while there appears to have been many attempted attacks against Ukrainian targets their actual effectiveness has been judged to be limited (as of June 2022).[83] A Microsoft report in late June 2022 pointed to the fact that only 29 per cent of cyber-attacks on IT systems in Ukraine, the US, Poland, and the

Baltic States "breached the targeted networks."[84] Either the attacks were thwarted or there appears to have been enough redundancy available to work around attacks that did reach their targets.[85] One possible reason for this lack of success is the fact that Ukraine's cyber defenses had been bolstered, both before and during the conflict, by Western state actors and private corporations, including Microsoft and Elon Musk's Starlink.[86]

There has also been little evidence of the use of AI-enhanced systems designed to generate cyber-psychological effects—such as the use of deepfakes (both video and voice)[87] and misinformation-spreading bots.[88] Moreover, the deepfake generated of Ukrainian President Volodymyr Zelensky at the beginning of the war, where he was 'seen' purportedly asking his troops to surrender, was not professionally produced. The next deepfake might, though, not be as easy to identify.[89]

However amateurish the deepfakes, the Microsoft report also noted that Russian offensive cyber seems to have been more effective in the cyber-psychological realm than in the cyber-technical. The spread of pro-Russian and anti-Ukrainian misinformation and disinformation across not just Ukraine but also the world at large is seen by this report to be a Russian success.[90] What was also noticeable was the coordination at times between cyber-technical and cyber-psychological attacks and actual kinetic strikes, which were designed to generate significant strategic effect.[91] This coordination was observed on several occasions, most notably when Russian missiles struck Kyiv's TV tower on March 1, 2022. Several cyber-attacks accompanied the strike on Ukraine's media companies. This combination of the use of offensive cyber and kinetic effect has been viewed as a multi-domain operation designed to have the strategic effect of generating chaos.[92] Also apparent has been the degree of Russian cyber espionage activity, especially against US systems. In this case, the help that Washington is providing to Ukraine in terms of cyber defense can only open Russian eyes to US cyber capabilities.[93]

But questions need to be asked about the employment of Russian offensive cyber when it comes to the Ukraine war. Why was it less apparent if the Russian military emphasized it before the conflict? Here it could be argued that there was a degree of underestimation of the target and a degree of hubris where its cyber capabilities were concerned.

There may, however, be other, more significant, issues at play. Admiral (Ret.) James Stavridis, the former Supreme Allied Commander of NATO forces, is wary of judging Russian offensive cyber based on the experience so far in Ukraine. He has noted that "Putin [is] saving massive scale non-deniable cyber-attacks for a later stage of the conflict." He says this would be in retaliation for when Western "sanctions really start to bite."[94] Another reason for the shortfall in effective cyber-technical interventions may be the Russian military not wanting to show its cyber hand. It is holding back on its true capabilities because of a concern over any future conflict with NATO itself. If such a conflict broke out, the military would want to create the aforementioned cyber *udar*. This shocking blow could render an immediate and overwhelming

effect on neutralizing adversary states. This shock value would be lost if NATO cyber defense specialists became aware of what Russian offensive cyber in the cyber-technical realm could do. These specialists could see where NATO's own vulnerabilities might lie and then take the necessary defensive action. NATO would be forewarned, and therefore, forearmed. Hence, the use of Russian offensive cyber as part of the Ukraine conflict may be limited because of the bigger strategic picture.[95] The Russian military might not want to waste perhaps the most effective weapon in its armory in the Ukraine conflict.

Thus, any analysis of the use of offensive cyber by the Russian military regarding the Ukraine conflict may not simply be a case of concluding that they are not as good as previously thought. It may not be as straightforward as this. There could be several rationales behind the lack of offensive cyber activities.

CONCLUSION

Russia's military hierarchy and its political leaders see their country as facing an existential threat from NATO and being geopolitically constrained by NATO power. The military has thus, for several years now, been on what amounts to a (albeit non-kinetic) war footing with core NATO states. The aim is to neutralize: to weaken NATO and its core states from within, and specifically to undermine their resolve to take any collective action against Russia. Offensive cyber is a crucial weapon in this war.

The predominant variant of offensive cyber used thus far has been the cyber-psychological: the long-term application of misinformation and disinformation to shape political opinions and to break the bonds of social cohesion. The cyber-technical form is also being used. There has been a continued Russian campaign involving cyber-espionage, reconnaissance, and the planting of malware. And, if international tensions do rise significantly, the Russian military—and making use of this preparatory work—may then engage in a series of massive cyberattacks designed to target the IT systems of NATO states. Again, after being subject to such an attack, these states might be in no position – or have the willingness – to take collective action against Russia.

In essence, offensive cyber offers the Russian military the chance to impose Russian will on its NATO adversary. It appears to have no other tool available in its armory that could do this. But just how effective can this offensive cyber option actually be? The experience of Ukraine would say that there may be little substance here, that the threat has been exaggerated. It is difficult, though, to draw too many conclusions from what has happened in Ukraine so far. The Russian military's offensive cyber capabilities, in cyber-psychological and cyber-technical forms, may yet prove to be very effective. Each does hold the promise of neutralizing NATO adversaries without necessarily inciting kinetic conflict. Beyond what is happening in Ukraine, Russian offensive cyber must be recognized as a latent and growing threat to NATO and its core states.

NOTES

1. United Kingdom Ministry of Defence. *Defence in a Competitive Age.* CP 411, March 2021,https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/974661/CP411_-Defence_Command_Plan.pdf.
2. Janis Berzins, "The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria," *Journal of Slavic Military Studies* 33, no 3 (2020): 355-80. DOI https://doi.org/10.1080/13518046.2020.1824109.
3. Elena Larina & Vladimir Ovchinskii, *Chas Volka: Vvedeniye v Khronopolitiku* [The Hour of the Wolf: Introduction to Chronopolitics] (Moscow: Knizhnyi Mir, 2019).
4. William Baxter, *Soviet Airland Battle Tactics* (Novato, CA: Presidio 1986), 10.
5. Simon Naveh, *In Pursuit of Military Excellence: The Evolution of Operational Theory* (London: Frank Cass, 1997), 172.
6. Konstantin Sivkov, "Pravo na Udar: Tol'ko Takaya Forma Vozdeystviya na Agressora Sorvet Ego Vozmozhnoye Voyennoye Vtorzheniye [A Right to Udar: Only Such a Form of Impact on the Aggressor Will Thwart his Possible Military Invasion]." *VPK.* Last modified March 3, 2014, https://vpk-news.ru/articles/19370.
7. Andy Greenberg, *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers* (New York: Anchor Books, 2020).
8. Andrei Soldatov & Irina Borogan, "The Man Behind Putin's Military," *Foreign Affairs.* Last modified February 26, 2022, https://www.foreignaffairs.com/articles/2022-02-26/man-behind-putins-military.
9. See Stephen Blank, "Cyber War and Information War a la Russe," in G. Perkovich and A. E. Levite (eds), *Understanding Cyber Conflict: Fourteen Analogies* (Washington DC: Georgetown University Press, 2017), 81-98; Jolanta Darczewska. "Russia's Armed Forces on the Information War Front," *OSW Studies*, no 57 (2016), https://www.osw.waw.pl/sites/default/files/prace_57_ang_russias_armed_forces_net.pdf; Greenberg, *Sandworm*; Scott Jasper, *Russian Cyber Operations* (Washington D.C.: Georgetown University Press, 2020); Bilyana Lilly & Joe Cheravitch. "The Past, Present and Future of Russia's Cyber Strategy and Forces," in T. Jancarkova, L. Lindstrom, M. Signoretti and I. Tolga (eds), *20/20 Vision: The Next Decade* (Tallinn: NATO, 2020), https://ccdcoe.org/uploads/2020/05/CyCon_2020_8_Lilly_Cheravitch.pdf; Frederick Westerlund, "Russian Intelligence Gathering for Domestic R&D – Short Cut or Dead End for Modernisation?" FOI Memo no. 3126. Stockholm: FOI Swedish Research Defense Agency, 2010.
10. Valerii Gerasimov, "Vektory Razvitiya Voennoi Strategii [Vectors of Military Strategy Development]," *Krasnaya Zvezda*, last modified March 4, 2019, http://redstar.ru/vektory-razvitiya-voennoj-strategii/.
11. S. Chekinov & S. Bogdanov, "O Kharaktere I Soderzhanii Voiny Novogo Pokoleniya [On the Character and Content of New-Generation Wars]," V*oennaya Mysl'* 22, no. 4 (2013): 13–24; A.V. Kartapolov, "Uroki Voennykh Konfliktov, Perspektivy Razvitiya Sredstv I Spocobov ikh Vedeniya. Pryamye I Nepryamye Deistviya v Sovremennykh Mezhdunarodnykh Konfliktov [Lessons of Military Conflicts and Prospects for the Development of Means and Methods for their Conduct. Direct and Indirect Actions in Contemporary International Conflicts]," *Vestnik Akademii Voennykh Nauk*, no. 2 (2015), http://www.avnrf.ru/index. php/zhurnal-qvoennyj-vestnikq/arkhiv-nomerov/737-vestnik-avn-2-2015; "Putin: Rossiya Vynuzhdena Otvechat' na Sozdaniye Ugrozy na Territorii Ukrainy Silami NATO [Putin: Russia is Forced to Respond to the Creation of Threats on Ukraine's Territory by NATO Forces]," Kommersant, last modified January 31, 2021, https://www.kommersant.ru/doc/5100337; Stephanie Pezard and Ashley L. Rhoades, *What Provokes Putin's Russia? Deterring Without Unintended Escalation* (Santa Monica, CA: RAND Corporation, 2020), https://www.rand.org/pubs/perspectives/PE338.html; "Putin's Munich Speech 15 Years Later: What Prophecies Have Come True?" TASS, last modified February 10, 2022, https://tass.com/politics/1401215.
12. Valerii Gerasimov, "NATO Ne Prigovor [NATO is not a Sentence]," *Voenno-Promyshlennyi Kur'er*, last modified April 30, 2019, https://vpk-news.ru/articles/49970; Kartapolov, "Lessons of Military Conflicts"; A.A. Kokoshin, *Voprosy Prikladnoi Teorii Voyny* [Questions of Applied Theory of War] (Moscow: Izdatels'kiy Dom VSHE, 2019); "Putin: Russia is Forced," Kommersant, 2021; V.N. Konyshev & A. Sergunin, *Sovremennaya Voennaya Strategiya* [Modern Military Strategy] (Moscow: Aspekt Press, 2014).
13. Ministry of Defense of the Russian Federation, *Voennaya Doktrina Rossiiskoi Federatsii* [Military Doctrine of the Russian Federation], Kremlin, last modified December 26, 2014, http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf.
14. Ministry of Defense of the Russian Federation, *Strategiya natsionalnoi bezopasnosti Rossiiskoi Federatsii* [National Security Strategy of the Russian Federation], Website of the Russian Security Council, last modified July 2, 2021, http://scrf.gov.ru/security/docs/document133/.

NOTES

15. Chekinov & Bogdanov, "On the Character and Content of New-Generation Wars"; Kartapolov, "Lessons of Military Conflicts"; Valerii Gerasimov, "Genshtab Planiruyet Udary [The General Staff Plans Strikes]," *Voenno-Promyshlennyi Kur'er* 9, no. 772, last modified March 12, 2019, https://vpk-news.ru/articles/48913; "Putin's Munich Speech 15 Years Later" TASS, 2022.
16. Chekinov & Bogdanov, "On the Character and Content of New-Generation Wars"; Kartapolov, "Lessons of Military Conflicts"; Richard Sokolsky, "The New NATO-Russia Military Balance: Implications for European Security," *Carnegie Endowmen*t, last modified March 13, 2017, https://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222.
17. Bryan Frederick, Matthew Povlock, Stephen Watts, Miranda Priebe & Edward Geist, *Assessing Russia's Reactions to U.S. and NATO Posture Enhancements* (Santa Monica, CA: RAND Corporation, 2017), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1800/RR1879/RAND_RR1879.pdf.
18. A.E. Sterlin & A.L. Khryapin, "Ob Osnovakh Gosudarstvennoi Politiki Rossiiskoi Federatsii v Oblasti Yadernogo Sderzhivaniya [On Foundations of Government Policy of the Russian Federation in Sphere of Nuclear Containment]," *Krasnaya Zvezda*, last modified August 7, 2020, http://redstar.ru/ob-osnovah-gosudarstvennoj-politiki-rossijskoj-federatsii-v-oblasti-yadernogo-sderzhivaniya; "Putin Rasskazal o 'Pervom Udare' I Vozmozhnosti Primeneniya Yadernogo Oruzhiya Rossiyei [Putin Spoke about the 'First Strike' and the Possibility of Using Nuclear Weapons by Russia]," *Sputnik Latvia*, last modified December 11, 2020, https://lv.sputniknews.ru/20201111/Putin-rasskazal-o-pervom-udare-i-vozmozhnosti-primeneniya-yadernogo-oruzhiya-Rossiey-14656937.html.
19. Gerasimov, "The General Staff Plans Strikes."
20. Rod Thornton, "Countering Prompt Global Strike: The Russian Military Presence in Syria and the Eastern Mediterranean and Its Strategic Deterrence Role," *Journal of Slavic Military Studies* 31, no. 1 (2019): 1-24, https://doi.org/10.1080/13518046.2019.1552655; "V Genshtabe Sochli Tselyu Kontseptsii SHHA 'Global'nyi Udar' Dominirovaniye v Mire [The General Staff considered the Goal of the US Concept 'Global Strike' to Be the Dominance of the World]," *Interfax*. Last modified Aug 7, 2020, https://www.interfax.ru/russia/720674; "Ugroza Global'nogo Udara SSHA Yavlyayetsya Osnovoi dlya Rossiiskoii VKO [The Threat of a US Global Strike Forms a Basis for Russian Air Space Defense]," *RIA Novosti.* Last modified April 4, 2015, https://ria.ru/20150404/1056636168.html.
21. Yakov Kedmi, "Moscow on the Euphrates," *Israel Defence*, No. 40 (Winter 2018).
22. Gerasimov, "The General Staff Plans Strikes"; Lyudmila V. Gundarova, "Kto Finansiruyet Tsvetnyye Revolyutsii na Postsovetskom Prostranstve [Who Finances Color Revolutions in the post-Soviet Space]," *Nezavisimoe Voennoe Obozrenie.* Last modified Jan 15, 2016, https://nvo.ng.ru/concepts/2016-01-15/1_revolutions.html; "S 'Tvetnykh Revolyutsiy' Hotyat Snyat' Kamuflyazh [They Want to Remove Camouflage from 'Color Revolutions']," Kommersant. Last modified April 3, 2015, https://www.kommersant.ru/doc/2679357; "Rossiya Obvinila NATO v Podgotovke 'Tsvetnykh Revolyutsiy' [Russia Blamed NATO for Preparing 'Color Revolutions]," *Lenta.* Last modified July 2, 2019, https://lenta.ru/news/2019/07/02/sovbez/.
23. V.N. Konyshev & R.V. Parfenov, "Gibridnye Voyny: Mezhdu Mifom y Real'nostryu [Hybrid Wars: Between Myths and Reality]," *Mirovaya Ekonomika y Mezhdunarodnye Otnosheniya,* no. 12 (2019): 56-66. http://liber.hse.perm.ru/absopac/app/webroot/index.php?url=/notices/index/IdNotice:93892/Source:default; MoD RF, *Military Doctrine of the Russian Federation 2014.*
24. (Col.) S. Chekinov & Lt-Gen. S. Bogdanov, "Asimmetrichnie deystviya po obespecheniyu voennoy bezopasnosti Rossii [Ensuring Russian military security by asymmetric means]," Voennaya mysl' no. 3 (2010): 13-22; (Col.) S. Chekinov & Lt-Gen. S. Bogdanov, "Vliyanie Nepryamykh Deystviy na Kharakter Sovremennoy Voyny [The impact of indirect methods on the nature of modern warfare]," *Voennaya mysl*' no. 6 (2011): 3-13; Chekinov & Bogdanov. "On the Character," 16–18; Kartapolov, "Lessons of Military Conflicts."

NOTES

25. Andrew Fatter, "Dialog o Strategicheskoi Stabil'nosti [Dialogue about Strategic Stability]," *Valdai Club*, last modified September 1, 2021, https://ru.valdaiclub.com/a/highlights/dialog-o-strategicheskoy-stabilnosti/; "Putin Nazval Dolyu Sovremennogo Yadernogo Oruzhiya [Putin named the fate of contemporary nuclear weapons]," *Regnum*, last modified August 23, 2021, https://regnum.ru/news/economy/3350979.html; "Oruzhiye Rossii: O Chem Putin Govoril v Poslanii Sovfedu [Russia's Weapons: What Putin spoke about in his message to the Federation Council]," *Ria Novosti.* Last modified April 22, 2021, https://crimea.ria.ru/20210422/Oruzhie-Putina-o-chem-prezident-govoril-v-poslanii-Sovfedu-1119496017.html; Markell Boystov, "Strategicheskaya Stabil'nost', Zderzhivanniye Ustrasheniyem I Yadernyi Simbioz [Strategic Stability, Containment through Deterrence, and Nuclear Symbiosis]," *Nezavisimoye Voyennoye Obozreniye.* Last modified September 2, 2021, https://nvo.ng.ru/armament/2021-09-02/1_1156_stability.html; "Rossiyane Polyubili Atomnuyu Bomby [Russians Learned to Love the Atomic Bomb]," *Vedomosti.* Last modified September 13, 2021, https://www.vedomosti.ru/society/articles/2021/09/13/886490-rossiyane-bombu.
26. Keir Giles & Mathieu Boulegue, "Russia's A2/AD Capabilities: Real and Imagined," *Parameters* 49, no. 1 (2019): 21-36. https://press.armywarcollege.edu/parameters/vol49/iss1/4/.
27. "NI: S-500 Obezpechit Pritsipal'no Novyi Uroven' Zashhity [NI: S-500 will Provide a Fundamentally Different Level of Protection]," *RG*. Last modified August 2, 2021, https://rg.ru/2021/02/08/ni-s-500-obespechit-principialno-novyj-uroven-zashchity.html.
28. United States Army, *The US Army in Multi-Domain Operations 2028*, TRADOC Pamphlet 525-3-1, 2018, https://api.army.mil/e2/c/downloads/2021/02/26/b45372c1/20181206-tp525-3-1-the-us-army-in-mdo-2028-final.pdf.
29. Yaacov Falkov, "Intelligence-Exalting Strategic Cultures: A Case Study of the Russian Approach," *Intelligence and National Security* 37, no. 1 (2022): 90-108, https://doi.org/10.1080/02684527.2021.1978135.
30. Maj-Gen. A. V. Serzhantov, "Transformatsiya Soderzhaniya Voiny: Ot Proshlogo k Sovremennomu [Transformation of the Concept of War: From Past to Present]," Voennaya Mysl', no 1 (2021), 58.
31. Gerasimov, "Vectors of Military Strategy"; Gerasimov, "The General Staff Plans Strikes."
32. Blank, "Cyber War and Information War a la Russe"; Sivkov, "A Right to Udar;" Rory Cormac & Richard Aldrich, "Grey is the New Black: Covert Action and Implausible Deniability," *International Affairs* 94, no. 3 (2018), https://warwick.ac.uk/fac/soc/pais/people/aldrich/secrets/inta94_3_01_cormac_aldrich.published.pdf.
33. Gerasimov, "Vectors of Military Strategy."
34. Thomas Rid, *Active Measures: The Secret History of Disinformation and Political Warfare* (London: Profile Books, 2020); A. Doronin, "Aktivnye Meropriyatiya: Informacionno-Psikhologicheskoe Vozdeistviye [Active Measures: Informational-psychological Influence]," *Agentura.* Last modified n.d. https://www.agentura.ru/equipment/psih/info/activ/; Maren Garberg Bredesen & Karsten Friis, "Missiles, Vessels and Active Defence," *The RUSI Journal* 165, no. 5-6 (2020): 68-78, https://doi.org/10.1080/03071847.2020.1829991; Dmitry (Dima) Adamsky, "From Moscow with Coercion: Russian Deterrence Theory and Strategic Culture," *Journal of Strategic Studies* 41, no. 1-2 (2018): 33-60, https://doi.org/10.1080/01402390.2017.1347872.
35. Gerasimov, "The General Staff Plans Strikes."
36. Rod Thornton & Marina Miron, "The Role of Aktivnost' Today in Russian Military-strategic Thinking and the Crucial Target of the 'Protest Potential of the Population," in *Russian Concept of Deterrence in Contemporary and Classic Perspective,* ed. Pentti Forsström (National Defence University, Department of Warfare, Series 2: Research Reports No. 11, 2021).
37. Doronin, "Active Measures."
38. Pavel Felgenhauer, "Dobitsya Prevokhodstva nad Ostol'nym Chelovechestvom [Achieving Superiority over the Rest of Humanity]," *Novaya Gazeta.* Last modified March 19, 2019, https://novayagazeta.ru/articles/2019/03/09/79808-dobitsya-prevoshodstva-nad-ostalnym-chelovechestvom.
39. Valerii Gerasimov, "Zennost' Nauki v Predvidenii [The Value of Science in Foresight]," *Voenno-Promyshlennyi Kur'er,* last modified February 26, 2013, https://vpk-news.ru/articles/14632.
40. Felgenhauer, "Achieving Superiority over the Rest of Humanity."
41. (Maj.) Yevgenii V. Safaryan, "Voennye Vyzovy I Ugrozy Dlya Rossiiskoii Federacii (Na Period 2030-2040 Godov) [Military Challenges and Threats to the Russian Federation: 2030-2040]," *Voennaya Mysl',* no. 4 (2021): 14-19.
42. Gerasimov, "Vectors of Military Strategy"; Gerasimov, "The General Staff Plans Strikes"; Thornton & Miron, "The Role of *Aktivnost'*"; Safaryan, "Military Challenges and Threats"; Serzhantov, "Transformation of the Concept of War."
43. Gerasimov, "Vectors of Military Strategy."

NOTES

44. V. M. Baryn'kin, "Minnoe Pole Informatsionnykh Voin [The Minefield of Information Warfs]," *Voenno-Promyshlennii Kur'er* [Military-Industrial Courier], no. 14 (2013); Chekinov & Bogdanov, "Ensuring Russian Military Security"; Chekinov & Bogadnov, "The Impact of Indirect Methods"; Gerasimov, "The General Staff Plans Strikes"; Konyshev & Sergunin, *Modern Military Strategy*; S. P. Rastorguyev, "Information Warfare as a Purposeful Information Impact of Information Systems," *Information Society*, Vol. 1 (1997). http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/5c8e75b6b46dfd0dc32575be00396796; S. P. Rastroguyev, *Formula Informatsionnoi Voyny* [Formula of Information War] (Moscow: Biblioteka Rasovoi Mysli, 1999).
45. Joseph S. Gordon, *Psychological Operations: The Soviet Challenge* (New York: Routledge, 1988).
46. Chekinov & Bogdanov, "On the Character;" Kartapolov, "Lessons of Military Conflicts;" Joe Gould and Mark Pomerleau, "Why the US Should Fight Russia, China in the 'Gray Zone'," *C4ISRNET*, last modified January 4, 2022, https://www.c4isrnet.com/information-warfare/2022/01/04/why-the-us-should-fight-russia-china-in-the-gray-zone/; Safaryan, "Military Challenges"; Clementine Starling, Tyson, Wetzel & Christian Trotti, "Seizing the Advantage: A Vision for the Next US Defense Strategy," Atlantic Council, last modified December 22, 2022, https://www.atlanticcouncil.org/content-series/atlantic-council-strategy-paper-series/seizing-the-advantage-a-vision-for-the-next-us-national-defense-strategy/.
47. Joan Prats I Amoros & Augustin Guillaume Barry, "Not Only Blood. The Need to Integrate Psychological Operations into the West's Military Culture," *Instituto Español de Estudios Estratagicos*, last modified September 19, 2019, https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEE81_2019JOAPRA_Psyops_ENG.pdf; Ivana Stradner, "The US Must Turn the Tables on Russia's Psyops," Defense One, last modified November 17, 2021, https://www.defenseone.com/ideas/2021/11/us-must-turn-tables-russias-psyops/186906/; Kier Giles, "The Next Phase of Russian Information Warfare," *NATO Strategic Communications Centre of Excellence,* last modified May 20, 2016, https://stratcomcoe.org/publications/the-next-phase-of-russian-information-warfare/176.
48. D. V. Galkin, P. A. Kolyandra & A. V. Stepanov, "Sostoyaniye I Perspektivy Ispol'zovaniya Iskysstvennogo Intellekta v Voennom Dele [Status and Prospects of Using Artificial Intelligence in Military Affairs]," *Voennaya Mysl',* no 1 (2021): 113-124.
49. A.A. Barthosh, "Gibridnaya, Skrytnaya, Nepredskazuyemaya [Hybrid, Covert, Unpredictable]," *Nezavisimoye Voennoye Obozreniye.* Last modified August 12, 2021, https://nvo.ng.ru/gpolit/2021-08-12/1_10_11_1153_hybrid.html.
50. Lilly & Cheravitch, "The Past, Present and Future."
51. Ibid.
52. Chekinov & Bogdanov, "On the Character"; Kartapolov, "Lessons of Military Conflicts"; Aleksandr Losev, "Voennii Iskusstvenii Intellekt [Military Artificial Intelligence]," *Arsenal Otechestva* 6, no. 32 (January 2018), http://arsenal-otechestva.ru/article/990-voennyj-iskusstvennyj-intellekt.
53. A.A. Barthosh, "Model Gibridnoi Voyny [The Model of Hybrid Warfare]," *Voennaya Mysl'*, Last modified May 1, 2019, https://vm.ric.mil.ru/Stati/item/191517; Chekinov & Bogadnov, "On the Character"; Valerii Gerasimov, "Mir Na Grane Voyny [The World on the Brink of War]," *Voenno-Promyshlenyi Kur'er* 10, no. 674, last modified March 15, 2017, https://vpk-news.ru/articles/35591; Gerasimov, "The General Staff Plans Strikes"; I. Panarin, SMI, *Propaganda I Informacionnye Voyny* [Media, Propaganda and Information Wars] (Moscow: Pokolenie, 2012); I. N. Vorobyov & V. A. Kiselyov, "Kiberprostranstvo kak sfera nepryamogo vooruzhennogo protivoborstva [Cyberspace as a sphere of indirect armed conflict]," *Voennaya Mysl'*, no. 12 (2014): 21-28.
54. Jasper, Russian Cyber Operations.
55. BBC Monitoring, "Russian Foreign Intelligence Chief Accuses West of 'Destructive interference,'" *BBC Monitoring,* last modified October 13, 2021, https://monitoring.bbc.co.uk/product/c202yc9o.
56. Vladimir A. Lefebvre, *Konfliktuyusshiye Struktury* [Conflicting Structures] (Moscow: Vysshaya Shkola, 1967); Vladimir A. Lefebvre, *Reflexive Control: The Soviet Concept of Influencing on Adversary's Decision Making Process* (Moscow: Science Applications, 1984); Timothy Thomas, "Russia's Reflexive Control Theory and the Military," *The Journal of Slavic Military Studies* 17, no 2 (2004): 237-256, https://doi.org/10.1080/13518040490450529.

NOTES

57. Lauriens Cerulus, "France Identifies Russia-linked Hackers in Large Cyberattack," Politico. Last modified February 15, 2021, https://www.politico.eu/article/france-cyber-agency-russia-attack-security-anssi/; Andreas Rinke & Kristi Knolle, "Russia Responsible for Cyber Attacks on German Parliament – German Foreign Ministry," *Reuters.* Last modified September 6, 2021, https://www.reuters.com/world/europe/russia-responsible-cyber-attacks-german-parliament-german-foreign-ministry-2021-09-06/; Christopher Bing, Joseph Menn & Raphael Satter, "Putin Likely Directed 2020 U.S. Election Meddling, U.S. Intelligence Finds," Reuters. Last modified March 16, 2021, https://www.reuters.com/article/usa-election-cyber-int-idUSKBN2B82PF; Dina Temple-Raston, "A 'Worst Nightmare' Cyberattack: The Untold Story of The SolarWinds Hack," *NPR,* last modified April 16, 2021, https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack?t=1635621136580.
58. United Kingdom Ministry of Defence, "Defence in a Competitive Age."
59. Ministry of Defence of the Russian Federation, *Military Doctrine.*
60. A.A. Barthosh, "Strategiya I Kontrastrategiya Gibridoi Voyny [Strategy and Counterstrategy of Hybrid War]," *Voennaya Mysl'*, no. 10 (2018): 5–19.
61. Evgenii Messner, *Khochesh' Mira, Pobedi Myatezhvoynu* [If You Want Peace, Win the Rebellion War] (Moscow: Military University Russkii Put', 2005).
62. Kokoshin, *Questions of Applied Theory of War.*
63. Konyshev & Sergunin, *Modern Military Strategy.*
64. Julian Barnes & Adam Goldman, "Russian Trying to Stoke Racial Tensions Before Election, Officials Say," *The New York Times,* last modified March 16, 2021, https://www.nytimes.com/2020/03/10/us/politics/russian-interference-race.html.
65. United Kingdom Intelligence and Security Committee, Russia Report (Intelligence and Security Committee of Parliament, 2020), https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.
66. Julian Borger, "When White Supremacist came to the US Capitol," *The Guardian,* last modified January 9, 2021, https://www.theguardian.com/us-news/2021/jan/09/us-capitol-insurrection-white-supremacist-terror; Ronald F. Inglehart, & Pippa Norris, "Trump, Brexit and the Rise of Populism; Economic Have-nots and Cultural Backlash," *Harvard Kennedy School Working Paper* (2016), https://formiche.net/wp-content/blogs.dir/10051/files/2017/01/RWP16-026_Norris.pdf.
67. Geir Hagen Karlsen, "Divide and Rule: Ten Lessons About Russian Political Influence Activities in Europe," *Humanities and Social Sciences Communications* (2019), https://www.nature.com/articles/s41599-019-0227-8.
68. Chekinov & Bogadnov, "Ensuring Russian military security"; Chekinov & Bogadnov, "The Impact of Indirect Methods"; Chekinov & Bogadnov, "On the Character;" Karatapolov, "Lessons of Military Conflicts."
69. Chekinov & Bogdanov, "On the Character."
70. Ibid.; Kartapolov, "Lessons of Military Conflicts."
71. Greenberg, *Sandworm*; Jasper, Russian Cyber Operations.
72. Rain Ottis, "Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective," *NATO CCDCOE*, last modified October 2018, https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf.
73. Greenberg, Sandworm; Colin Demarest, "Blue, Yellow and Grey Zone: The Cyber Factor in Ukraine," *C4ISRnet*, last modified March 14, 2022, https://www.c4isrnet.com/cyber/2022/03/14/blue-yellow-and-gray-zone-the-cyber-factor-in-ukraine/.
74. United Kingdom National Cyber Security Centre, "Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed," *NCSC.gov*. Last modified October 3, 2018, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed; United States Cybersecurity and Infrastructure Agency, "Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders," CISA.gov, last modified April 26, 2021, https://us-cert.cisa.gov/ncas/alerts/aa21-116a.
75. Heather Conley & Jean-Baptiste Jeangene Vilmer, "Successfully Countering Russian Electoral Interference," *CSIS Briefs*, last modified June 21, 2018, https://www.csis.org/analysis/successfully-countering-russian-electoral-interference.
76. Greenberg, Sandworm; Jasper, *Russian Cyber Operations.*

NOTES

77. "Russian Cyber Units," *Congressional Research Service*, last modified February 2, 2022, https://crsreports.congress.gov/product/pdf/IF/IF11718c; Greenberg, Sandworm; Westerlund, "Russian Intelligence Gathering;" Josephine Wolff, "Understanding Russia's Cyber Strategy," *Foreign Policy Research Institute*, last modified July 6, 2021, https://www.fpri.org/article/2021/07/understanding-russias-cyber-strategy/.
78. Larina & Ovchinskii, *The Hour of the Wolf;* "Kiberataki Strashnee, Chem Yadernoye Oruzhiye: Kak Mirovye SMI Otreagirovali na Virus Petya [Cyberattacks are Scarier than Nuclear Weapons: How the Global Media Reacted to the Petya Virus]," TASS, last modified June 29, 2017, https://tass.ru/mezhdunarodnaya-panorama/4374732.
79. Thornton & Miron, "The Role of *Aktivnost'*"; Vasilii Kashin, "Vliyanie Kiberoruzhiya na Strategicheskuyu Stabil'nost' v XXI Veke [The Impact of Cyber Weapons on Strategic Stability in the 21st Century]," Carnegie Endowment for International Peace, last modified December 27, 2018, https://carnegie.ru/commentary/78033; Galkin, Kolyandra & Stepanov, "Status and Prospects of Using Artificial Intelligence;" D. V. Galkin & A.V. Stepanov, "Voprosy Bezopasnosti Primeneniya Iskusstvennogo Intellekta v Sistemakh Voennogo Naznacheniya [Security Questions of the Use of AI in Military Systems]," *Voennaya Mysl'*, no. 4 (2021): 72-79.
80. Losev, "Military Artificial Intelligence."
81. Ryan Browne, "The world is bracing for a global cyberwar as Russia invades Ukraine," CNBC, last modified February 25, 2022, https://www.cnbc.com/2022/02/25/will-the-russia-ukraine-crisis-lead-to-a-global-cyber-war.html.
82. Eric Tegler, "The vulnerability of AI systems may explain why Russia isn't using them extensively in Ukraine," *Forbes*, last modified March 16, 2022, https://www.forbes.com/sites/erictegler/2022/03/16/the-vulnerability-of-artificial-intelligence-systems-may-explain-why-they-havent-been-used-extensively-in-ukraine/?sh=5ecf559837d5
83. Raphael Satter, Christopher Bing, and James Pearson, "Microsoft Discloses Onslaught of Russian Cyber Attacks on Ukraine," *Reuters*, last modified April 27, 2022, https://reuters.com/technology/microsoft-discloses-onslaught-russian-cyberattacks-ukraine-2022-04-27/.
84. "Defending Ukraine: Early Lessons from the Cyber War," Microsoft, last modified June 22, 2022, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.
85. David E. Sangar & Julian Barnes, "Many Russian Cyber Attacks Failed in First Months of Ukraine War, Study Finds," *The New York Times*, last modified June 22, 2022, https://www.nytimes.com/2022/06/22/us/politics/russia-ukraine-cyberattacks.html.
86. Christopher Miller, Mark Scott, and Bryan Bender, "UkraineX: How Elon Musk's Space Satellites Changed the War on the Ground," *Politico*, last modified June 8, 2022, https://www.politico.eu/article/elon-musk-ukraine-starlink.
87. Philip Oltermann, "European politicians duped into deepfake video calls with the mayor of Kyiv," *The Guardian*, June 25, 2022, https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko?amp;amp.
88. Tegler, "The vulnerability of AI systems may explain why Russia isn't using them extensively in Ukraine."
89. Tom Simonite, "A Zelensky Deepfake Was Quickly Defeated. A Next One Might Not Be," *WIRED,* last modified March 17, 2022, https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/.
90. "Defending Ukraine."
91. Satter, Bing, and Pearson, "Microsoft Discloses."
92. Danyil Martinyak, "'Unprecedented' Cyberattack Blamed on Russia Was Meant to Sow Chaos in Ukraine," *Asia News*, last modified February 17, 2022, https://central.asia-news.com/en_GB/articles/cnmi_ca/features/2022/02/17/feature-01; Clare Roth, "Ukraine Cyberwar Creates Chaos, 'It Won't Win the War,'" *Deutsche Welle,* last modified March 3, 2022, https://www.dw.com/en/ukraine-cyberwar-creates-chaos-it-wont-win-the-war/a-60999197.
93. Sean Lyngaas, "Microsoft Says Russia Has Stepped Up Cyber Espionage Against the US and Ukraine Allies," CNN, last modified June 22, 2022, https://edition.cnn.com/2022/06/22/politics/microsoft-russia-hackings/index.html.
94. Catherine Philp, "Putin armed cyberattack aimed at me, says former MI6 chief," *The Times*, last modified May 26, 2022, https://www.thetimes.co.uk/article/putin-aimed-cyberattack-at-me-says-former-mi6-chief-sir-richard-dearlove-xtlq83cql.
95. Jaspreet Gill, "Russia May Be Holding Cyber Capabilities In Reserve, So U.S. Must Keep Its Shields Up: Experts," *Breaking Defence*, last modified March 14, 2022, https://breakingdefense.com/2022/03/russia-may-be-holding-cyber-capabilities-in-reserve-so-us-must-keep-its-shields-up-experts/.