Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy

by
James J. Wirtz

Chapter 3 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

In Chapter 3, James J. Wirtz, Dean of the Naval Postgraduate School in California, describes the global context surrounding these events. Today, nation-states are integrating cyber tactics into their political and military strategies. Professor Wirtz posits that when it comes to the use of cyber, 'national styles' might be emerging as states attempt to use cyber capabilities to achieve strategic objectives. He suggests that it is wrong to treat cyber attacks as a silver bullet, and that it is better to consider how a sort of combined arms approach will prevail. On a positive note, the need for legal and bureaucratic integration of policies and programmes should produce national idiosyncrasies on the cyber battlefield that can help with the vexing challenge of attribution.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy

James J. Wirtz
Naval Postgraduate School

Discussion of the cyber domain in general, and specific considerations of cyber attacks, cyber war and cyber power, often seem oddly detached from a broader strategic and geopolitical context.[1] Several reasons can be suggested for why the cyber dimension of conflict seems to be considered in isolation from the *physical and political* goals that states and non-state actors attempt to achieve through their activities in the virtual world of cyberspace. Offensive and defensive cyber capabilities are highly classified by all parties; it is impossible to say with certainty what capabilities are wielded, making it difficult to assess 'cyber orders of battle' and 'cyber balances of power'. Newspaper reports, anecdotes, and rumours of capabilities offer clues, but it is difficult to link rumours to grand strategic objectives. Cyber warfare is an exquisitely technical subject dominated by engineers, mathematicians, and computer scientists – individuals who can be forgiven for focusing on the latest patch needed in some software program, and for not thinking about the connection between technical exploitation and grand political strategy. In a sense, issues related to cyber warfare are often treated, not just as something technically new on the military landscape, but as something that is unprecedented in military affairs.

If one turns a strategist's eye toward the cyber domain, key questions immediately emerge. How will states integrate their cyber capabilities into an overall strat-

1 The opinions here are not those of the U.S. Navy, U.S. Government or the North Atlantic Treaty Organisation.

egy to achieve military and political goals? In other words, no matter how brilliant the algorithm, no matter how devious the penetration, how can cyber power be integrated into a 'combined arms' or even a 'whole of government' approach leading to battlefield success or to a grand strategy that creates a political *fait accompli*? Unless one embraces the dubious proposition that cyber really constitutes the ultimate silver bullet in political and military conflict, it is unlikely to be employed independently as a war-winning weapon. Moreover, given the need for integration, issues of political and strategic culture, to say nothing of bureaucratic preferences and peacetime legal restraints, can be expected to produce national styles and preferences when it comes to conflict in cyberspace.[2]

> *Political and strategic culture produce national styles and preferences in cyberspace.*

Although attribution of known cyber attacks remains a hotly contested and much denied issue (given the very limited evidence available), there is some indication that strategic culture and organisational preferences shape the way the United States, China and Russia use their cyber power. According to press reports, the United States was behind the Stuxnet malware attack on centrifuges at Iran's Natanz enrichment facility.[3] Many analysts suggested at the time that the Stuxnet attack was noteworthy as the first example of the use of a cyber weapon to cause physical damage, but it also reflected the long-standing American tradition of long-range precision bombardment and the preference for targeting key nodes in an opponent's infrastructure to produce maximum damage with minimal effort.[4] By contrast, the recent Office of Personnel Management hack, which press reporting attributes to the People's Republic of China, seems to reflect a Chinese preoccupation with guarding its own citizens from nefarious outside influences, while going to great lengths to gather information that is locked behind others' defensive barriers.[5]

Russian cyber activities, especially those associated with the recent conflict in Ukraine and the annexation of Crimea, probably offer the best example of the employment of cyber attacks to shape the overall political course of a dispute. According to David J. Smith:

---

2 According to Colin Gray, 'The political context of strategy is exceedingly broad. It includes the domestic political and bureaucratic processes by which strategy is made and amended…all strategies are contrived and executed by people and institutions that must be considered encultured by the societies that bred them.' Colin Gray. *The Strategy Bridge: Theory for Practice* (Oxford: Oxford University Press, 2010). pp. 39-40.

3 Ellen Nakashima and Joby Warrick. 'Stuxnet was work of U.S. and Israeli experts, officials say,' *Washington Post*, June 2, 2012. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html; David E. Sanger. 'Obama Ordered Sped Up Wave of Cyberattacks Against Iran,' *The New York Times,* June 1, 2012, p. A1. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyber-attacks-against-iran.html.

4 Lawrence Freedman. *The Evolution of Nuclear Strategy,* (3rd edition, New York: Palgrave MacMillan, 2003), pp. 11-12; Michael E. Brown, *Flying Blind: The Politics of the U.S. Strategic Bomber Program* (Ithaca: Cornell University Press, 1992), pp. 29-67.

5 Sean Lyngaas. 'Exclusive: The OPM breach details you haven't seen,' *Federal Computer Week* August 21, 2015. http://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx; Jon R. Lindsay. 'The Impact of China on Cybersecurity: Fact and Friction,' *International Security*, Vol. 39, No. 3 (Winter 2014/2015), pp, 7-47.

> *Russia holds a broad concept of information warfare, which includes intelligence, counterintelligence, deceit, disinformation, electronic warfare, debilitation of communications, degradation of navigation support, psychological pressure, degradation of information systems and propaganda. Computers are among the many tools of Russian information warfare, which is carried out 24 hours a day, seven days a week, in war and peace. Seen this way, distributed denial of services attacks (DDoS), advanced exploitation techniques and Russia Today television are all related tools of information warfare.*[6]

Russia, more than any other nascent actor on the cyber stage, seems to have devised a way to integrate cyber warfare into a grand strategy capable of achieving political objectives.

> *Russia seems to have devised a way to integrate cyber warfare into grand strategy.*

The remainder of this essay explains what it is about Russian strategic culture that enables it to wield cyber power in a strategically effective manner. It begins with a brief discussion of Russian strategic culture, especially how it manifested in past debates the impact of technology on warfare. It then describes how Russia has employed its cyber power to defeat US and NATO deterrence strategies, effectively delivering a strategic defeat to the alliance at the outset of its 'hybrid' war against Ukraine. The essay concludes by offering some observations about the strategic nature of cyber warfare.

1 Russian Strategic Culture and Technology

Often, states or individuals who initially invent or master some new technology fail to understand, not only its strategic implications, but also how best to employ it in a tactical or operational setting. Historically, Russia, including its Soviet manifestation, has not been at the forefront of scientific or technical innovation. As one recent history explained, Soviet Cold War espionage was largely dedicated to stealing scientific, technical, and military information from the West in a desperate and ultimately failed effort to keep pace with more sophisticated and innovative opponents.[7] Nevertheless, while the Russians may lack in technological prowess and innovative drive, they tend to excel in their ability to foresee the broad impact of technology on the battlespace. Several sources can be suggested as the basis of this talent. As Robert Bathhurst explained decades ago, the Russians tend to be 'dreamers', allowing

6 David J. Smith. 'How Russia Harnesses Cyberwarfare,' *Defense Dossier*, Issue 4, August 2012, pp. 7-8.

7 According to Michael Warner, 'Soviet spies were crucial to keeping the USSR alive and competitive for two reasons: they stole enough industrial secrets to substitute for innovation in some sectors, and they kept Moscow apprised of where the West was reading Soviet secrets,' Michael Warner. *The Rise and Fall of Intelligence: An International Security History* (Washington, D.C.: Georgetown University Press, 2014), p. 161.

their imaginations to run wild and envision the implications of technology.[8] In the 1920s, for instance, Soviet writers were thinking about supersonic dogfights on the fringes of space – something that has not occurred nearly a century later. During the Cold War, visions of a fully functioning Star Wars missile defence system shook the Kremlin to its foundations, despite the fact that even proponents of Reagan-era missile defence recognised that many of the components of the system were at the outer fringes of technical feasibility. In other words, while America focuses on issues of technology and systems integration, Russia tends to leap immediately to considerations of the strategic implications of emerging weapons systems.

> *America focuses on technology, Russia tends to leap to the strategic implications of weapons systems.*

A second influence that shapes Russian views of emerging technology is the fact that, in their hearts, they are good Clausewitzians. In other words, they understand the paramount nature of politics in war. War is a political act. Its purpose is to alter the political judgments of opponents to better suit our own interests. Thus, to have a strategic effect, cyber power must be used in a way that will shape the political outcome of war. Russians are thus quick to think through the links between technology, military operations, strategy, and ultimately political outcomes, despite their lack of technological dexterity. Soviet estimates of the military balance, for example, reflected a broad assessment of the so-called 'correlation of forces', which incorporated political and economic trends, not just force ratios based on 'bean counts' of military units. Soviet alarm over NATO's 1983 Able Archer exercise, for instance, was greatly influenced by the political rhetoric emanating from the Reagan White House, not by some fundamental shift in the military balance in Europe. The Russian officer corps, especially in Soviet days, was also encouraged to think through the strategic implications of new technologies. Today, the Russian Army provides senior officers with multiple venues to debate not only doctrine, but theory. By contrast, US officers, who tend to focus on operational matters, generally lack similar venues to assess the strategic and political implications of new technology.[9] In fact, many analysts point to a 2013 article signed by the Chief of the Russian General Staff, *The Value of Science in Anticipating* as laying out the Russian way of cyber warfare.[10]

A fine illustration of these phenomena is the emergence of the concept of 'Military-Technical Revolution,' more commonly referred to by Western analysts as the

8 Robert B. Bathurst. *Intelligence and the Mirror* (London: Sage, 1993).

9 For a recent discussion of how operational considerations, for instance, take centre stage in what is purportedly Naval strategy see Peter D. Haynes. *Toward a New Maritime Strategy: American Naval Thinking in the Post-Cold War Era* (Annapolis: Naval Institute Press, 2015).

10 Valery Gerasimov. 'The Value of Science in Anticipating [in Russian], Military-Industrial Courier, February 27, 2013, quoted in Matthew Rojansky and Michael Kofman. 'A Closer look at Russia's 'Hybrid War'," *Wilson Centre Kennan Cable* , No 7, April 2015, p. 3.

'Revolution in Military Affairs.'[11] By the mid-1970s, NATO defence planners recognised that they confronted a serious challenge along the Central Front. If war broke out in Europe, NATO would do well against first-echelon Warsaw Pact formations, but the Alliance could only slowly bring reinforcements across the Atlantic. Soviet third-echelon forces – units made up mostly of inactive reservists in peacetime – would probably defeat NATO because they would reach the battle before reinforcements streaming across the Atlantic. The United States and its allies had to prevent the third-echelon of the Red Army from reaching the Forward Edge of the Battle Area (FEBA). The solution to the third-echelon threat was found in several new technologies that would allow NATO to conduct precision strikes against Warsaw Pact staging areas, depots, transportation hubs, and armoured formations hundreds of miles behind the FEBA. By the mid-1980s, US programmes known as Assault Breaker and Smart Weapons Program, and NATO initiatives called Emerging Technologies and Follow on Forces Attack, were integrated into a new US Army Air-Land Battle doctrine, creating a nascent reconnaissance-strike complex. US planners adopted a rather nonstrategic and apolitical view of these new technologies – they simply saw them as a way to stop Soviet third-echelon forces from reaching the Central Front.

By contrast, the Soviets now anticipated a 'Military-Technical Revolution', predicting that the emerging reconnaissance-strike complex would transform conventional combat, producing truly strategic and political effects. Soviet strategists believed that long-range precision strikes could destroy forces and critical supply, communication, and command nodes deep within the enemy's rear, creating conditions for a catastrophic theatre-wide collapse. Put somewhat differently, the system of systems possessed by the Americans and their NATO allies would rob the Warsaw Pact of its ability to mass and manoeuvre forces, or even to conduct combined arms operations. Soviet officers estimated that the nature of war was about to change: conventional, not nuclear, munitions might soon become the weapon of choice against massed armoured and infantry formations. They saw the potential impact that this emerging system of systems could have on strategy, war, and international politics; there was a real possibility that the Warsaw Pact could be rendered militarily and politically ineffective by these emerging weapons and ways of war.

Ironically, Soviet predictions of a Military-Technical Revolution set off alarm bells in the West, as analysts scrambled to detect the new secret Soviet weapon that would produce these revolutionary developments in war. Americans were slow to realise that the Soviets were in fact writing about American weapons, and the nascent precision-strike complex, which was in fact possessed exclusively by the United States and the NATO alliance. As a result, many of the key concepts related to the application of information-age technologies in warfare were produced by Soviets thinking about the weapons systems being deployed by their opponents, and not by the more technically competent Americans.

11 Dima Adamsky. *The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the US and Israel* (Stanford: Stanford University Press, 2010).

2 Russian Cyber Strategy

Today, how is this Clausewitzian-inspired Russian strategic imagination being applied to the use of cyber power? The answer can be found by first exploring the strategic challenge they apparently believe they face: the NATO alliance. NATO is based on the concept of collective defence that enhances its strategy of deterrence. Through formal agreements and long-standing and extensive collaboration, NATO sends a strong signal that member states will stand together in the face of threats to collectively deter aggression against its members. The objective of this deterrent policy is to preserve the peace. This is a key observation. The goal of NATO's deterrent strategy is to reduce or even eliminate the possibility of war by ensuring that aggressors understand *ex ante* that an attack against one of its members is an attack against the entire Alliance. Especially today, NATO primarily exists to prevent war, not to develop enhanced strategies or capabilities to prosecute war or to wield forces to achieve ancillary objectives. In a sense, NATO exists to preserve the peace and to make sure that changes to the status quo in Europe occur through political processes that lead to the spread of democracy, the rule of law, and adherence to international norms. The *raison d'être* of NATO is to preserve the peace; the purpose behind its strategy is to deter war.

To achieve its objective – rapid change of the European status quo to better fit their Russia-centric, not democratically-cantered, interests and preferences – Russia opted to pick a course of action not to defeat NATO, but to defeat NATO's *strategy*. By presenting the Western alliance with a *fait accompli* through actions that produce minimal death and destruction, Russia attempted to shift the onus of escalation onto NATO, thereby inflicting a strategic defeat on the Alliance at the outset of hostilities or even in the event of non-democratic changes to the status quo. Russia is banking on the hope that NATO will either be incapable or unwilling to transform this strategic defeat into active conventional combat, which would further undermine NATO's goal of preserving the peace. In effect, the Russians seem to have realised that by defeating NATO's strategy at the outset of a confrontation, they can actually alter political perceptions within the Alliance in a way that suits their objectives. Put somewhat differently, the risk of a forceful NATO response to some provocation is minimised by keeping the death and destruction associated with any *fait accompli* to an absolute minimum. NATO is especially vulnerable to cyberattacks and information warfare because Russia can undermine NATO's deterrent strategy without causing casualties. NATO has the option of reversing the *fait accompli*, but the required level of death and destruction simply highlights the failure of its deterrent strategy.

> *Russia opted to pick a course of action not to defeat NATO, but NATO's strategy.*

Cyber power, as a key facet of hybrid warfare, is an important enabler in an attack on NATO's deterrent strategy.[12] Cyber attacks are not specifically targeted to eliminate key nodes, but to intensify the fog of war by sowing confusion within command and control networks and NATO polities. For instance, according to press reports, Russian movement into the Ukraine was accompanied by myriad cyber attacks, including Distributed Denial of Service (DDoS) tactics against computers in Kyiv, Poland, the European Parliament, and the European Commission.[13] If local political and military leaders cannot develop an accurate estimate of quickly developing events, critical hours or even days can be gained with which Russia can create facts on the ground that can only be reversed at great effort. A little bit of 'sand in the works', so to speak, is enough to further delay the relatively slow-pace of decision-making in the West.[14]

Cyber power is an important enabler in an attack on NATO's deterrent strategy.

The annexation of Crimea also began with a series of covert operations that used a disinformation campaign to create ambiguity and delay Ukraine's response, effectively extending the element of surprise achieved by the Russian gambit. According to Michael Kofman and Matthew Rohansky:

> *'Russia's use of broadcast tools for propaganda and psychological operations, part of a broader information campaign to support the Crimean annexation, caught both the Ukraine and the West by surprise. Moscow amped up the alarmist content of its broadcasting . . . stoking fear and confusion in Crimea'.*[15]

Admittedly, the annexation was completed using more traditional operations involving conventional units, but the cyber-enabled opening moves not only allowed Russia to test the Western response, but to buy the time needed to create a *fait accompli* through conventional means.

Western analysts have noted that even though the Crimea crisis surprised the West, the Russian effort to integrate television and the internet, especially various

12 As Michael Kofman and Matthew Rojansky note, 'hybrid warfare,' including the Russian variations used against the Ukraine is not unique. The point here, however, is that Russia is particularly adept as using cyber power in the practice of hybrid warfare; see Kofman and Rojansky, (*op cit*) p. 2. Other analysts have noted how the Crimea annexation and the additional actions against Ukraine were dependant on capabilities long under development that were especially crafted not to trigger a NATO response; Aleksandr Golts and Heidi Reisinger. 'Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence,' Research Paper No 105 (Research Division – NATO Defence College Rome) November 2014.

13 Owen Matthews. 'BIG READ: Russia leading the way in the cyber arms race,' *Irish Examiner*, Saturday June 13, 2015. www.irishexaminer.com'lifestyle'feature'big-read-russia-leading-the-way-in-the-cyber-arms-race-336675.html.

14 The key point is that information denial or dominance does not have to be absolute, it just needs to foster delay and uncertainty in Western political and military decision-making. According to Paul Saunders, 'Russia's seizure of Crimea happened very quickly. U.S. and European decision-making processes just don't move at that speed, particularly when facing ambiguity. Once a Crimea-style operation has begun, it will be extremely difficult if not impossible for Western decision-makers to be sufficiently confident about the other side's intent to take consequential action before it's too late'; Saunders, P. 'Why America Can't Stop Russia's Hybrid Warfare,' *The National Interest* June 23, 2015. www.nationalinterest.org/feature/shy-america-can't-stop-russias-hybrid-warfare-13166.

15 Kofman and Rojansky, p. 4.

types of social media, into its effort to shape opponents' political perspectives, has been ongoing for quite some time. In a sense, Russia has worked hard to use the internet to shape the political environment of conflict: it has (1) developed internally and externally focused media with a significant online presence; (2) used social media to guarantee that Russian narratives reach the broadest possible audience; and (3) polished their content in terms of language and presentation so that it rings true in various cultural settings.[16] These activities have recently been given their own moniker – trolling – the practice of creating cyber actors with false identities to communicate tailored messages to an unsuspecting audience.[17] According to Keir Giles:

> *'Russian assessments of current events makes it clear that Russia considers itself to be engaged in full-scale information warfare, involving not only offensive but defensive operations – whether or not its notional adversaries have actually noticed this is happening'*.[18]

What most analysts fail to realise, however, is that Moscow has shaped this cyber-enabled information warfare in a very strategic manner. Cyber power is being wielded as a strategic weapon to create facts on the ground with the minimal use of kinetic force.

3 Conclusion

Because of its rather inchoate nature, the cyber domain is a milieu in which various strategic cultures can be manifest. Russian strategic culture focuses on war as a political activity; for cyber power to have a truly strategic effect, Russia believes that it must contribute directly to shaping political outcomes by altering the political perceptions of their opponents to better suit their interests. If one also accepts the idea that Russians are especially adept at understanding the political and strategic impact of new technologies, it is possible that they have grasped the real strategic opportunities created by the information revolution – opportunities that might be given short shrift by analysts shaped by different strategic cultures.

The true test of strategy, however, is found in a specific geopolitical and military context. In terms of Crimea and Ukraine, the Russians have developed an exquisite strategic application of cyber power not to defeat NATO's military capabilities, but to defeat NATO's strategy by creating a *fait accompli* while sidestepping NATO's deterrent. By using cyber power to create 'facts on the ground' with minimal casual-

16 Keir Giles. 'Working Paper: Russia's Hybrid Warfare: a Success in Propaganda,' European Security and Defence College, 18 February 2015. www.baks.bund.de'de'aktuelles/working-paper-russias-hybrid-warfe-a-success-in propaganda
17 Adrian Chen. 'The Agency,' *New York Times Magazine*, June 2, 2015. p. 57.
18 Giles.

ties, they shifted the onus of escalation onto NATO to reverse the *fait accompli*. In a sense, they created a situation in which NATO leaders must choose between suffering a harsh strategic defeat (the eruption of war in Europe) and the accommodation of the Russian annexation of Crimea and ongoing pressure against Ukraine. Cyber power, either in the form of direct attacks or a concerted information campaign, was used to create this dilemma for NATO by delaying a Western response until these stark choices emerged. The lesson is clear: if one can defeat an opponent's strategy, then it is possible to achieve one's objectives without defeating an opponent's forces or triggering execution of a deterrent threat.