5 Cyber War and Information War à la Russe

STEPHEN BLANK

Originally this chapter was to explore an analogy between cyber warfare and Russia's traditional conception and practice of information warfare (IW). However, an examination of Russian strategy, argumentation, and practice in Estonia, Georgia, and Ukraine between 2006 and 2016 demonstrates that the relationship between cyber warfare and IW is not analogous but rather something more. Russia has integrated cyber and information warfare organically into its planning and capabilities to project power. As the US director of National Intelligence Gen. James Clapper testified in 2015, before the cyber attack on the Ukrainian electricity sector, Russia was establishing a cyber command to conduct

> offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems. Russia's armed forces are also establishing a specialized branch for computer network operations.
>
> Computer security studies assert that unspecified Russian cyber actors are developing means to access industrial control systems (ICS) remotely. These systems manage critical infrastructures such as electric power grids, urban mass transit systems, air traffic control, and oil and gas distribution networks. These unspecified Russian actors have successfully compromised the product supply chains of three ICS vendors so that customers download exploitative malware directly from the vendors' websites along with routine software updates, according to private sector cybersecurity experts.[1]

Clearly, Russian national security agencies are preparing for contingencies in the cyber domain as much as their counterparts in the United States, China, Israel, the United Kingdom, France, and other states are. What may be distinctive in Russia, as the examples presented in this chapter suggest, is the conception of cyber attacks as an organic element of a long-standing approach to political warfare and information operations (IO).

In Russian discussions and practice, distinguishing cyber war from IO is virtually impossible.[2] For Moscow they both come under the heading of attributes of information confrontation (Informatsionoye protivoborstvo [IP]), or IW, and are

to be fully integrated in any campaign with military operations.[3] Beginning with Chechnya in 1999–2000 and through the conflicts in Estonia, Georgia, and Ukraine, Moscow has systematically employed its concepts of IW.[4] As is discussed in the following sections, the December 2015 malware assault that shut down several Ukrainian electricity transmission facilities was the most vivid example.

Russian conduct of both IW and cyber war builds on earlier foundations of what George Kennan called political warfare.

> Political warfare is the logical application of Clausewitz's doctrine in time of peace. In broadest definition, political warfare is the employment of all the means at a nation's command, short of war, to achieve its national objectives. Such operations are both overt and covert. They range from such overt actions as political alliances, economic measures (as ERP [European Recovery Plan]—the Marshall Plan), and "white" propaganda to such covert operations as clandestine support of "friendly" foreign elements, "black" psychological warfare and even encouragement of underground resistance in hostile states.[5]

Tactics and strategies developed and employed during the Soviet period have served as a foundation for establishing new strategies that incorporate some of the century-old Leninist repertoire and new trends like IW, as defined by Moscow, for the conduct of continuous political warfare against hostile targets. Although some Russian and foreign observers use new terms such as "nonlinear" or "new generation" warfare to describe Russia's practice and often say they merely mimic techniques used by the United States to interfere in other states, the IW that Russia conducts today follows the logic of past Soviet and Russian political warfare.

This chapter sketches those historical patterns and explores how newer forms of cyber operations fit into them, drawing on the experiences of Estonia in 2007, Georgia in 2008, and Ukraine in 2014–15.[6] For Russia, cyber operations may represent new forms of military operations, but they have grown organically out of Soviet thinking and tactics about political warfare.[7] This observation raises, among other things, the question of whether Russia regards and treats cyber capabilities differently than do other states and, if so, how these differences might be managed if not reconciled. It also may suggest that states will tend to utilize new technologies, including cyber, according to familiar strategies, cultural, and institutional predilections.

Russia's Permanent Siege Mentality

Russian national security policy begins with the perception that Russia lives in a constant state of siege that includes intelligence operations and the overall national security challenges posed by adversaries that are led by the United States. As Christopher Andrew and Vasili Mitrokhin wrote about the Soviet regime's abiding mind-set, "All authoritarian regimes, since they regard opposi-

tion as fundamentally illegitimate, tend to see their opponents engaged in subversive conspiracy." President Vladimir Putin and his associates, like their forebears, have frequently expressed their belief that the conspiracies directed against them are mainly foreign in origin.[8]

In Russia, there is no hard-and-fast distinction between peace and war as there is in American strategic thinking. The US military has a concept of "phase zero," or the stage antecedent to war. Rather, given its perception of permanent and protracted conflict, Russia is every day preparing for war by deploying all the instruments of state power globally to enhance its security and interests.

Observing the operations of Russian state and associated criminal actors on a day-to-day basis demonstrates that the entire Russian state participates in political warfare, IW, and actual military operations. Russian official documents on national security since 2009 have all been plans for mobilizing the entire state for conflict.[9] If one reads the 2009 document and the 2015 national security strategy and tracks behavior of the regime since 2009, then it becomes clear that the entire state is being put on a mobilization footing. Not only do they systematically reinforce the message that Russia is under attack from both US-led IW and military threats but also the regime has allocated massive resources to spend on information operations like Russia Today and "troll factories" in Russia.[10] Defense spending and the industry it supports are portrayed as locomotives of economic growth as well as security measures.[11]

The instruments by which Russia conducts its operations are fundamentally nonmilitary and represent a Russian version of the term "whole of government." Although Moscow is clearly willing to use force as in Georgia and Ukraine, those military operations represent the culmination (or at least the intended culminating point) of a strategy premised on years-long operations using coordinated nonmilitary instruments and military threats to subvert targeted governments from within. In other words, IW, which includes cyber warfare, saturation of the media, and psychological operations, is intended to achieve the results that direct force would otherwise have to accomplish. Just as some Russian commentators maintain that the end of the Cold War and even the US occupation of Germany and Japan after 1945 were massive information operations leading to strategic victories without firing a shot, they maintain that properly conducted IW can give Moscow much, or all, of the victory it currently seeks at much lower cost. To the extent that hostile interventions in other states cannot be certainly attributed to Russia, Moscow can avoid or complicate any reprisals by its adversaries. And given that cyber operations do not rise to a level of violence that the North Atlantic Treaty Organization (NATO) regards as "military operations," NATO leaders are hesitant to respond.[12]

The concepts underlying these operations evolved in response to the fiscal, moral, and intellectual trauma that the Soviet and Russian military establishments experienced from at least 1991–2000 due to the discrediting effects of their opposition to reform and their malfeasance in the First Chechen War between 1994 and 1996. The Russian establishment saw the United States and NATO as mounting an unstoppable threat to its interests and identity as an imperial great

power. NATO enlargement, the 1998–99 war in Kosovo, and Western support for the democratization of former Soviet states manifested this threat and intensified Russia's feeling of being under siege. In the Second Chechen War, from 1999 to 2007, Moscow effectively insulated the Russian information space from outside influence. Since Russian elites clearly believed that the loss of domestic public support during the First Chechen War was a major factor in Russia's defeat, they were determined to prevent that from happening again. State efforts to curtail media access and reporting in the Second Chechen War ensured that popular support for Russia's military operations would be staunch and enduring. The government waged a systematic campaign to capture Russian hearts and minds, recognizing that target as the true center of gravity. Public support was an invaluable lubricant of the armed forces, and a media campaign was mounted to mobilize that public support, to isolate the insurgents from domestic and foreign support, and to frame the war as an antiterrorist campaign.[13] Enduring public support allowed Putin to give the military a freer rein to fight a long war without any hint of public opposition. Russia's effective insulation of the theater and of the Russian media space demonstates how important control of the media and of the "narrative," or "framing," is to any war-winning strategy. This tactic enabled Russia to pursue and conduct sustained and vicious operations that included the use of thermobaric weapons, among other instruments.[14]

Building on the brutal success of the second Chechen campaign, Putin sought to rethink contemporary warfare and rebuild an effective military. If the United States is seen as the world's dominant military power with its array of sophisticated weapons platforms, the challenge is to find ways for Russia to win on different terms. It should not be surprising that the current strategy, much like that of 1921–39, identifies surrogate forms of power to compensate for deficiencies in sophisticated armaments. Thus, asymmetric war, including IW and IO, gained adherents because it increasingly seemed a safe alternative at much lower cost than direct military confrontation with NATO or the United States, given Russia's economic inferiority and military shortcomings. Russian writers also clearly believed that Russia itself was under information attack and that retaliation was obviously justified.[15] Moreover, the lack of enemy capabilities for definitive attribution and the fact that information warfare tools could be used like a thermostat, with the temperature being constantly adjusted as needed, lowered the risk to Russia.

The analogy to the Soviet period here is quite striking. As Jonathan Haslam has observed, "Special operations were used by the Soviet Union against prewar Poland. So special operations, or war by other means, were very much a feature of the 1920s, which was also a time of relative Soviet military weakness. Asymmetrical activities with covert operations were a substitute for not having the use of direct military power."[16]

Indeed, in 2007 Defense Minister Sergei Ivanov suggested,

> The development of information technology has resulted in information itself turning into a certain kind of weapon. It is a weapon that allows us to

> carry out would-be military actions in practically any theater of war and most importantly, without using military power. That is why we have to take all the necessary steps to develop, improve, and, if necessary—and it already seems to be necessary—develop new multi-purpose automatic control systems, so that in the future we do not find ourselves left with nothing.[17]

The creative adaptation of earlier concepts and practices has proven useful to Moscow. Despite its strategic inferiority vis-à-vis the United States and NATO, Russia has won every war in which it has participated since 2000. Its successful use of IW in all these operations attests to its improved grasp of how information and cyber operations (which are a unified phenomenon in its thinking) contribute to victory.

Estonia

In 2007 the Estonian government moved a statue commemorating the Soviet Union's liberation of Estonia in World War II, defying Russian threats of reprisal if it did so. Immediately, Russians in Estonia demonstrated en masse. A widespread cyber attack was launched on Estonia's essential information and computer technology infrastructure: banks, telecommunications, media outlets, and name servers.[18] The offensive included denial of service, botnets, hacking, and systematic attacks on government offices, banks, and communications networks.[19] This "war" lasted from April 26, 2007, until mid-May 2007.

While these attacks were occurring, Moscow instituted sanctions on Estonia, demanded a revision of its laws concerning its Russian minorities, and called it a fascist or pro-fascist regime.[20] Moscow organized violent demonstrations in Tallinn among the Russian diaspora there. Meanwhile, the Russian youth organization Nashi (Ours) demonstrated at the Estonian Embassy in Moscow. This organization, like other such youth groups in Russia, is a creation of the Putin regime. Moscow has also employed Nashi and similar groups against other foreign embassies and domestic dissidents.[21]

The use of botnets precludes definitively identifying the source of attacks. Yet, although the cyber attack on Estonia cannot be conclusively traced to the Russian government, the available evidence is overwhelming: it was a predesigned Russian attack. Duma deputy Sergei Markov, a frequent Russian governmental spokesman, boasted in 2009 that his assistant and office were behind the attacks and that more such events would happen.[22] (President Putin has admitted that he began planning the Georgian war of 2008 in 2006. Estonia may possibly have been a cyber dress rehearsal for that war as well as a probe of Estonian defenses and NATO's response.[23])

Estonian authorities' investigation of the April–May 2007 incidents revealed that planning for the demonstrations and cyber strikes in Tallinn began in 2006, or well before any sign that the monument would be removed, which was the ostensible pretext for the Russian attack.[24] "They were planned in advance and

at least somewhat coordinated, as Russian-language forums were full of the preparations and planning in the days leading up to the attacks. The Estonian government even planned to release news of the strike three days before it began but was dissuaded by the European Union (EU) because of an upcoming meeting between then EU president and German chancellor Angela Merkel and Russian president Vladimir Putin."[25] Indeed, in a 2006 article, Russian scientists forecast the exact nature of how botnets would be used to achieve denial of service in targeted computers.[26]

Estonian authorities observed that the demonstrations in Tallinn resembled earlier tactics and efforts by Soviet and Russian Federation authorities to destabilize or even unseat governments deemed insufficiently friendly or obedient—for example, the Czechoslovak and Bulgarian governments in postwar Europe.[27] Estonian authorities recorded the presence of Russian special forces in civilian clothes at the demonstrations, though it is not clear which of the many different kinds of the Russian special forces they meant.[28]

By disrupting and possibly unhinging the Estonian government and society, and by demonstrating NATO's incapacity to protect Estonia against this novel form of attack, the cyber attacks aimed to compel Estonia to consider Russian interests in its policies. In other words, it had a classically Clausewitzian objective of bending the enemy—Estonia, in this case—to Russia's will. In Estonia, as perhaps in the later case of Georgia, the attack may have reflected not only an effort to correct Estonia's behavior or influence its orientation but also a desire to punish it and deter others from following suit by making it an example of the risks to anyone who crosses Russia.[29]

Estonian authorities (and others) believe that Russia aimed to incite large enough demonstrations that they would provoke violence. Then, they argue, Moscow could have used the ensuing violence as a pretext for launching an anti-Estonian insurgency that could have justified either direct Russian support for the insurgents or even Russian military intervention, as occurred in Crimea in 2014. Though Western audiences might consider such threat assessments and scenarios far-fetched, the Estonians and other neighbors of Russia do not. The resemblances to earlier Soviet operations, the nature of the attacks, and the foreshadowing of the Crimean operation are more than suggestive. Indeed, the use of disaffected ethnic minorities and anger at the Baltic states' "lack of gratitude for independence" are long-standing Russian and Soviet tactics as are the organization of minority or other mass demonstrations.[30] Of course, it is inherent in the nature of cyber operations that they frequently cannot be definitively attributed to a particular source. It is but one aspect of their value.

A main goal of hybrid war—including its information and cyber dimensions—is to instill a feeling of constant political and economic insecurity among the target state's population. This pressure—in the form of trade wars, energy blackmail, propaganda, diplomatic deceit, and coercion to join alternative regional integration projects—has been felt by the post-Soviet states of the EU Eastern Partnership: Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine. Since their independence most of the Eastern Partnership states have felt that they

live in an insecure environment because of existing frozen conflicts, among other reasons. In this region, hybrid warfare aims less at the security and more at the stability of the region. In such conditions, the desire for stability is intense and can easily be manipulated. The campaign's main idea is that there is no stability without Russia.[31]

In the words of Estonian defense minister Jaak Aaviksoo, "It is true to say that the aim of these attackers was to destabilize Estonian society, creating anxiety among people that nothing is functioning, the services are not operable. This was clearly psychological terror in a way."[32] This observation confirms John Arquilla's insight: "Terror has been a part of war for a long time, and many centuries ago began to slip the bonds of the national and/or imperial 'monopolies' on its practice. Beyond this sense of its lasting presence in history, there are also abundant signs of terror's conceptual similarity with war as we have generally conceived of it for millennia."[33]

Another strategic purpose of the cyber operation against Estonia, as perceived by Estonian authorities, was to test to what degree European security institutions like the EU, NATO, and the Council of Europe would stand by the country. In this regard, Estonians say, Russia not only was surprised to find the strong if somewhat belated response by the EU and Council of Europe but was also disappointed by the lack of support by Russians living in Estonia.[34] However, NATO's response was late in coming. This also could have been instructive to Moscow and its neighbors.

Moving from Russia's strategic objectives to its operational practice, new forms of IW or of large-scale influence buying can be seen as updated analogues of Soviet ideological warfare and subvention of foreign communist parties and their media after 1921 that was intended to keep enemies "off balance." This strategy often involves the collaboration of Russia's largely state-owned energy firms, intelligence agencies, organized crime, and embassies in buying up key businesses in targeted states; in donating funds to political movements and politicians, thereby compromising them; and in general exercising a covert influence on local politics. This strategy informs Russian policy from the Baltic to the Black Sea and in the war against Ukraine.[35] This strategy goes beyond Russia's tense relations with its neighbors and encompasses the potential for waging such war farther afield against hostile governments in Europe and elsewhere or as part of an insurgency within a state.

Cyber attacks may play a role as needed in implementing such a strategy or may be self-standing operations in their own right that can be endlessly repeated and turned on or off. Indeed, the cyber attacks on Estonia occurred within the context of Russia's unyielding efforts to exploit the energy dependencies of all three Baltic states—Latvia, Lithuania, and Estonia—and used the combination of energy monies, bought and subverted politicians, intelligence penetration, and organized criminal syndicates to exert constant pressure on the Baltic, East European, and Central Asian states.[36]

In Estonia and in subsequent manifestations of IW and IO, the Russian government has cooperated with organized crime structures such as the Russian Business

Network (RBN) to launch attacks. According to researchers Eli Jellenc and Kimberly Zenz:

> RBN is a cyber crime organization that ran an Internet service provider (ISP) until 2007 and continues to be heavily involved in cyber crime such as phishing, malware distribution, malicious code, botnet command and control, DDOS [distributed denial of service] attacks, and child pornography. . . . While it is not certain that RBN is directly connected to the Russian mafia, it is highly likely. RBN is heavily involved in child pornography, which is traditionally controlled by the Russian mafia, and its official leader, who goes by the alias "Flyman," is suspected of running those operations (and of possibly being a pedophile himself). It is also known that Flyman has family connections to the government: his father or uncle was involved in politics in St. Petersburg before taking an important position at a ministry in Moscow. Another RBN member, Aleksandr Boykov, is a former lieutenant colonel in the *Federalnaya Sluzhba Bezopasnosti* (FSB, the successor agency to the KGB). While it is currently not possible to prove that RBN has worked in tandem with the FSB or other security services (collectively, the *siloviki*), it is likely that they are at least connected.
>
> When RBN officially hosted Internet services between early 2006 and November 2007, it was linked to 60 percent of all cyber crime.[37]

RBN may have suspended its operations since 2007. But cybercrime has grown significantly since 2007 and has spread across numerous ISPs. Therefore, cybersecurity experts continue to use the term "RBN" to refer to the loosely organized group of cyber criminals based in Russia, and cyber activity and crime by this group continue to remain high.[38]

The Estonian case reflects the logic of political warfare and its information warfare components that have long been part of Soviet and Russian strategy and practice. While the post-communist era brought changes, including the prominence of criminal syndicates and the use of unofficial groups such as hacktivists, the tactic of exerting coercive pressure on neighboring nations and states is not new. One year after the cyber attacks on Estonia, Georgia experienced a similar campaign.

Georgia

In Georgia Russia first attempted to combine kinetic and cyber attacks against command-and-control and weapons systems on the one hand, and information-psychological attacks against media, communications, and perceptions on the other hand. In other words, Russia organically integrated what Western sources would consider cyber attacks into a broader information and military operation. Although the results were mixed, the Russian political-military leadership has deeply studied this campaign and sought to refine for future use the tactics used

in both aspects of its IW campaign against Georgia. Richard Weitz of the Hudson Institute observed,

> The techniques used by the Russian attackers suggest they had developed a detailed campaign plan against the Georgian sites well before the conflict. The attackers did not conduct any preliminary surveying or mapping of sites [which might have prematurely alerted Georgian forces], but instead immediately employed specially designed software to attack them. The graphic art used to deface one Georgia Web site was created in March 2006 but saved for use until the August 2008 campaign. The attackers also rapidly registered new domain names and established new Internet sites, further indicating they had already analyzed the target, written attack scripts, and perhaps even rehearsed the information warfare campaign in advance.[39]

Capt. Paulo Shakarian noted similarly that beyond the direct attacks on Georgian state institutions, the cyber campaign was part of a larger information battle between Russian media and the Georgian and Western media for control of the narrative. Here Russian bloggers were able to flood a CNN-Gallup poll with posts stating that Russia's cause was justified, and attempted to prevent Georgian media from telling Tbilisi's story.[40] In the early stages Russian "hacktivists" shut down the websites of Georgia's president, Ministry of Defense, Ministry of Foreign Affairs, Parliament, National Bank, the English-language online news dailies *The Messenger* and *Civil Georgia*, and the online Rustavi 2 television channel while also defacing the websites of the Ministry of Foreign Affairs and the National Bank.[41]

In the Georgia war of 2008, clearly Russian proficiency at IW had substantially improved from the Estonian operation. Russian military commanders, working with hackers, in both cases directed computers from locations throughout the world to attack Estonian and Georgian sites, thereby creating botnets.[42] Other studies underscore the sophistication of the IOs directed against Georgia. Most attacks were actually carried out by civilians with little or no direct (or certainly traceable) involvement by the Russian government or military. These cyber attackers were recruited through the Internet and social technology. As in Estonia, attackers were aided by Russian organized crime even to the point of hosting software ready for use in other cybercrime activities. The organizers of the cyber attacks seem to have had advance notice of Russian military intentions and were tipped off about the timing of Russian military operations while they were taking place. The absence of reconnaissance or mapping of sites at the onset of the operation signified that Russian intelligence had already deeply penetrated the Georgian networks. The number of attackers working against Georgia was much greater than those who had attacked Estonia even though far fewer computers were involved.[43] Jeff Carr, an investigator for Project Grey Goose, an organization of a hundred American volunteer security experts from the private and government sector, concluded that "the level of advance preparation and reconnaissance

strongly suggests that Russian hackers were primed for the assault by officials within the Russian government."[44]

The first wave of cyber attacks on August 6–7, 2008, was carried out by botnets and command-and-control systems that were associated with Russian organized crime. Twenty-four to forty-eight hours later, Russian military operations commenced. Afterward, the second wave hit mainly, though not exclusively, through postings on websites, again a carryover from Estonia. These postings contained both the cyber attack tools and the lists of suggested targets to attack. Although cyber attacks were limited to denial of service and website defacements, which are relatively unsophisticated types of attacks, they were carried out in a very sophisticated manner.[45] Once Russian troops had established positions in Georgia, the attack list expanded to include many more websites of government agencies, financial institutions, business groups, educational institutions, news media, and a Georgian hacking forum to preclude any effective or organized response to the Russian presence and to induce uncertainty regarding what Moscow's forces might do. These attacks significantly degraded the Georgian government's ability to deal with the invasion by disrupting communications between it and Georgian society, by stopping many financial transactions, and by causing widespread confusion. It is also possible that spyware and malware were inserted into the Georgian systems for future criminal or military-strategic use.[46] The clear objective of the cyber strikes was to support and further the goals of the Russian military operations as they were timed to begin on a large scale within hours of the first Russian military strike. The attacks ended just after those operations did.

Subsequent reporting found that cyber attacks on Georgian websites and online discussions of upcoming military operations began weeks before the actual onset of hostilities. Such preparatory action included a "dress rehearsal" of the upcoming cyber attacks, providing further evidence of the unprecedented synchronization of cyber with all other military combat actions.[47] The comparative restraint in not attacking key infrastructural targets—including energy installations—but demonstrating the ability to do so, both in Georgia and beyond, signaled a broader strategy to deter Georgia or others from escalating the conflict.[48]

This last point is particularly important. Simultaneously displaying the capacity to destroy key infrastructural targets while withholding orders to do so makes an impression on both the directly targeted states and the interested but heretofore uninvolved observers. Those observers could, of course, ultimately become targets themselves. Restraint in exercising coercive options aims to de-escalate the conflict by simultaneously conveying moderate Russian intentions while demonstrating Russia's potential to do more harm, thereby deterring the target and third parties from retaliating.

The Georgian IW campaign highlights the returns that Moscow gained on its substantial investment in the resources needed to conduct IO and IW. Moscow struck to prevent Georgian accession to NATO and prove Russia's primacy in the former Soviet space, and it seems to have achieved both objectives. In addition, the Georgian war highlighted Russia's advancing cyber capabilities.

Crimea and Eastern Ukraine

Russia's interventions in Crimea and Eastern Ukraine, beginning in 2014, followed the patterns of the 2007 and 2008 exertions in Estonia and Georgia. The greater duration and intensity of the Ukraine conflict reflects the deeper political-economic connections between Russia and Ukraine and the greater stakes Russia perceives in repelling Western influence over Ukraine's future. Russian leaders perceived the onset of the crisis—that is, the demonstrations against Viktor Yanukovych's government—and the subsequent departure of Yanukovych as a coup conducted with, at least, the collusion of the West. As such, the situation provided stark confirmation of the Kremlin's portrayal of existential US-led hostility to Russian interests.

As in Estonia, Russian actors mounted intense IO to shape how Ukrainians, Russians, and international audiences perceived the unfolding events. These operations were conducted through all media, especially Web-based outlets. Opinion surveys and anecdotal reporting in Russia indicate the effectiveness of these efforts in shaping perceptions in Russia (if not elsewhere).[49] For example, a 2014 Levada Institute survey found that 69 percent of Russians believed that this media provided "an objective picture" of the crisis in Ukraine. A full 88 percent believed the United States and the West were "conducting an information war against Russia."[50] In June 2015 the Pew Research Center found that 50 percent of Russians blame the West for the conflict in Ukraine.[51] Russia also mounted economic pressure on Ukraine and on western European states and consumers who rely on energy inputs flowing through Ukraine. Connections between the Russian state, businesses, individual elites, and their Ukrainian counterparts also were exploited to solidify both Russia's hold on Crimea and the pro-Russian elements' hold on parts of Eastern Ukraine.

NATO's Cooperative Cyber Defence Centre of Excellence published an account of the cyber war in Ukraine through November 2015.[52] It demonstrates the occurrence of cyber strikes and IW against Ukraine's revolution in 2013–14 as well as during the war, though not at the level that had occurred earlier in Estonia and Georgia, where the denial of service and disruption attacks were largely seen as "symbolic" in nature.[53] In Ukraine investigations revealed a Russian cyber campaign known as Operation Armageddon, which reportedly began in mid-2013. According to a US cybersecurity firm, attackers used spear-phishing emails with attachments that appeared official to lure Ukrainian officials and other high-level targets. Malware then infected the victims' computers and was used to "identify Ukrainian military strategies" in order to advance Russian war objectives.[54]

In July 2014 a pro-Russia hacktivist group reportedly hacked into one of Ukraine's largest commercial banks and published stolen customer data on a Russian social media website. Earlier the bank's co-owner had offered a $10,000 bounty for the capture of Russian-backed militants in Ukraine. The circumstances and rudimentary quality of this operation left some commentators doubting a link to Russian state authority.[55] The same hacktivist group entered

the Ukrainian Finance Ministry network in May 2015 and posted what it claimed were documents stolen from the network that revealed Ukraine was unable to service its external debt.[56] Seen from a different angle, these activities amount to an electronic campaign to prepare the battlefield.

If the information operations in Ukraine through late 2015 resembled those in Estonia and Georgia earlier, a new and more forceful application occurred on December 23, 2015, when sophisticated cyber attacks shut down three regional electric power distribution companies, affecting approximately 225,000 customers. As an investigative report of the US Department of Homeland Security recorded, these synchronized and coordinated attacks were conducted remotely, exploiting legitimate credentials of Ukrainian operators "via unknown means." Multiple human actors remotely hijacked the operation of breakers at more than fifty regional substations. According to the department's report, "The primary access pathway was the use of legitimate remote access pathways such as VPN [virtual private network] to access local systems. . . . The exact nature of the credential harvesting remains unknown. It is likely that the credentials were obtained well ahead of the December 23, 2015, event."[57]

The deep knowledge and advanced penetration of the Ukrainian electricity providers follow the patterns seen in Estonia and Georgia. In the Ukrainian conflict, given the deeper ongoing human connections with Russia, it is possible that human agents and collaborators were involved. In any case, the cyber attack reflected strategic thinking and operational planning, befitting Russia's articulated general approach to information warfare. Importantly, in this regard, while the preparations for the attack were begun well in advance—perhaps shortly after the deposition of the Yanukovych government in February 2014—the attack itself was unleashed one month after Ukrainian nationalists and Crimean Tartars disabled electricity transmission lines to Crimea, beginning on November 22, 2015.[58] The Crimean total power outage lasted two weeks.[59]

Thus, if the cyber attack on Ukraine was instigated directly or indirectly by Russian authorities, then it suggests a strategic logic that also was seen in Georgia, where capabilities to attack the energy infrastructure were put in place but not activated. In Georgia the Georgian state did not escalate the conflict, and Western powers did not intervene. Russian cyber operators did not then have cause to attack Georgia's energy supply system. Conversely, the attack on the energy supply to Russian-held Crimea was, in Russian eyes, an escalation that invited a somewhat symmetrical response. Ukraine's energy supply was cut off—the symmetrical part—but the method was a sophisticated cyber penetration and attack when compared to the simple toppling of transmission towers. Taken together, the Georgian and Ukrainian examples reflect a logic of deterrence and compellence by cyber means. A capability to do harm is emplaced to deter adversaries from acting against Russian interests. When the adversary is restrained, the cyber attack is not unleashed, but when the adversary attacks Russian interests, Russian actors inflict a roughly proportionate response.

Conclusion

The Russian deep state clearly has incorporated cyber strikes and information operations into information warfare, as it defines the term. IW assumes growing importance as a war-winning strategy that avoids attribution, inhibits enemy reactions, and minimizes expenses—all crucial strategic issues for Russia. These trends in IW also appear to Russia's leaders as an equal and opposite, if possibly asymmetric, reaction to what they believe is an all-encompassing political and information war being conducted against them and Russia.[60]

Russia's government thus defines IW as a strategic war-winning force in its own right and as an indispensable weapon for the intelligence preparation of the battlefield over many years. The ensuing subversion of the enemy from within, before a shot is fired, is an essential strategic operation. Other countries' military and political leaders appear to overlook these points at their own and our allies' peril. The instruments themselves may not be new, but their combination and the uses for which they are deployed strongly diverge from Western thinking and practice. Russia's strategy and operations in the information and cyber warfare domain continue to confound Western governments and audiences who have yet to devise a compelling strategy with which to meet Russia's exertions.[61]

Dismissing Russia's view as paranoid may be emotionally satisfying, but it leaves the rest of the world ill prepared for actual cyber war, which for Russia is a constant ongoing phenomenon whether direct force is being used or not. To paraphrase Leon Trotsky, we may not be sufficiently interested in differing views about IW like Russia's, but Russia's view of IW is very interested in us. Russia has already engaged its adversaries in information warfare; thus, its adversaries must understand and learn from it for their own security.

Notes

All of the foregoing was written before the final months of the 2016 US presidential election. Russian information warfare operations in the US campaign followed the logic and patterns of episodes recounted in this chapter and require a separate analysis.

1. James R. Clapper, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Armed Services Committee, February 26, 2015, http://fas.org/irp/congress/2015_hr/022615clapper.pdf, 2–3.

2. Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2015); Roland Heickerö, *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations* (Stockholm: Swedish Defense Research Agency, 2013), www.foi.se; and Tim Thomas, "Russian Strategic Thought and Cyber in the Armed Forces and Society: A Viewpoint from Kansas," presentation at the Center for Strategic and International Studies, Washington, DC, January 20, 2016.

3. Thomas, "Russian Strategic Thought."

4. Geers, *Cyber War in Perspective*; and Stephen Blank, "Russian Information Warfare as Domestic Counterinsurgency," *American Foreign Policy Interests* 35, no. 1 (2013): 31–44.

5. Max Boot and Michael Doran, "Political Warfare," Policy Innovation Memorandum no. 33 (Washington, DC: Council on Foreign Relations, June 2013), http://www.cfr.org/wars-and-warfare/political-warfare/p30894.

6. Stephen Blank, "Class War on the Global Scale: The Culture of Leninist Political Conflict," in *Conflict, Culture, and History: Regional Dimensions,* ed. Stephen Blank et al. (Maxwell Air Force Base, AL: Air University Press, 1993), 1–55.

7. Ibid.; Maria Snegovaya, *Putin's Information War in Ukraine: Soviet Origins of Russia's Hybrid Warfare*, Russia Report I (Washington, DC: Institute for the Study of War, 2015); and Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, no. 2 (2004): 237–56.

8. See Christopher Andrew and Vasili Mitrokhin, *The Sword and the Shield: The Mitrokhin Archive and the Secret History of the KGB* (New York: Basic Books, 1999), 31. They explicitly tie this insight to the Bolshevik Party from the moment it took power until its demise in 1991.

9. Stephen Blank, "'No Need to Threaten Us, We Are Frightened of Ourselves': Russia's Blueprint for a Police State—the New Strategy," in *The Russian Military Today and Tomorrow: Essays in Memory of Mary Fitzgerald*, ed. Stephen J. Blank and Richard Weitz (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, 2010), 19–150; "Military Doctrine of the Russian Federation"(Washington, DC: Carnegie Endowment for International Peace, February 5, 2010), www.carnegieendowment.org/files/2010russia_militarydoctrine.pdf ; "Military Doctrine of the Russian Federation, February 5, 2010," Foreign Broadcast Information Service–Central Asia (FBIS-SOV), February 9, 2010; Voyennaia Doktrina Rossiiskoi Federatsii, December 26, 2014, www.kremlin.ru; *Natsional'naya Strategiya Bezopasnosti Rossii, do 2020 Goda* (Moscow: Security Council of the Russian Federation, May 12, 2009), www.scrf.gov.ru, and available in English from FBIS-SOV, May 15, 2009, in a translation from the Security Council website (henceforth NSS); and *Natsional'naya Strategiya Bezopasnosti Rossii*, December 31, 2015, www.kremlin.ru.

10. Russia Today, a Russian news agency, is widely considered as acting as the voice of the Kremlin. The channel receives funding from the Russian government, which Russian president Vladimir Putin acknowledged in a June 2013 comment: "Certainly the channel is funded by the government, so it cannot help but reflect the Russian government's official position on the events in our country and in the rest of the world one way or another." A sizable portion of its budget comes from the Russian government, including a reported $307 million in 2016. For more, please see Max Fisher, "In Case You Weren't Clear on Russia Today's Relationship to Moscow, Putin Clears It Up," *Washington Post*, June 13, 2013, https://www.washingtonpost.com/news/worldviews/wp/2013/06/13/in-case-you-werent-clear-on-russia-todays-relationship-to-moscow-putin-clears-it-up/?utm_term=.a2ca4bb6d35e; and "Russia Cuts State Spending on RT News Network," *Moscow Times*, October 11, 2015, https://themoscowtimes.com/articles/russia-cuts-state-spending-on-rt-news-network-50194.

11. "Russia Cuts State Spending," *Moscow Times*; Blank, "'No Need to Threaten Us,'" 19–150; Andrew Monaghan, "Defibrillating the Vertikal? Putin and Russian Grand Strategy" (London: Chatham House, October 7, 2014); Presentations by Kirill Rogov and Sergei Aleksashenko at the German Marshall Fund, Washington, DC, April 25, 2015; "Russian Military Production Up by Nearly 20% in 2015," Sputniknews.com, April 19, 2016; Steven Rosefielde, "Russia's Military Industrial Resurgence: Evidence and Potential," paper presented to the Conference on the Russian Military in Contemporary Perspective, Washington, DC, May 9–10, 2016; and Aleksandr Bastrykin, "Pora Postavit'

Deistvennyi Zaslon Informatsionnoi Voine," April 18, 2016, http://www.kommersant.ru/doc/296157816.

12. Vladimir Vasilyevich Karyakin, "The Era of a New Generation of Warriors—Information and Strategic Warriors—Has Arrived," *Nezavisimaya Gazeta Online*, Moscow (in Russian), April 22, 2011, Open Source Committee, FBIS-SOV, September 11, 2012; M. A. Gareyev, "Russia's New Military Doctrine: Structure and Substance," *Military Thought* no. 2 (2007): 1–14; and Y. N. Baluyevsky, "Theoretical and Methodological Foundations of the Military Doctrine of the Russian Federation (Points for a Report)," *Military Thought* no. 1 (2007): 15–23, exemplify this point.

13. Blank, "Russian Information Warfare."

14. Ibid.

15. Karyakin, "Era of a New Generation"; Gareyev, "Russia's New Military Doctrine"; and Baluyevsky, "Theoretical and Methodological Foundations."

16. Quoted in Thomas K. Grose, "Russia's Valuable Weapon: Vladimir Putin's Spies Are Critical to His Strategy in Syria and Ukraine," *U.S. News & World Report*, October 14, 2005, http://www.usnews.com/news/the-report/articles/2015/10/14/russias-spies-are-critical-to-putins-operations-in-syria-ukraine.

17. Sergei Ivanov, NTV, Moscow (in Russian), August 15, 2007, Open Source Center, FBIS-SOV, August 15, 2007.

18. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, August 21, 2007, 163.

19. A concise description of the attacks may be found in Rebecca Grant, *Victory in Cyberspace* (Washington, DC: US Air Force Association), 3–9.

20. James A. Hughes, "Cyber Attacks Explained," *CSIS Commentary* (Washington, DC: Center for Strategic and International Studies, June 15, 2007).

21. Stephen Blank, "Towards the Police State: Increasing Authoritarianism in Putin's Russia," *Acque e Terre* no. 4 (2007).

22. William J. Dobson, *The Dictator's Learning Curve: Inside the Global Battle for Democracy* (New York: Random House, 2012), 31.

23. "Putin Admits Moscow Planned Military Actions in Georgia in Advance," Rustavi 2, Tbilisi, August 8, 2012, http://www.rustavi2.com/news/news_text.php?id_news=46258&pg=1&im=main.

24. Conversations with Estonian authorities in Tallinn, October 2007.

25. Gadi Evron, "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War," *Georgetown Journal of International Affairs* 9, no. 1 (Winter/Spring 2008): 122–23.

26. Igor Kotenko and Alexander Ulanov, "Agent-Based Modeling and Simulation of Network Softbots' Competition," in *Proceedings of the Seventh Joint Conference on Knowledge-Based Software Engineering*, ed. Enn Tyugu and Takahira Yamaguchi (Amsterdam: IOS Press, 2006), 243–52.

27. Conversations with Estonian authorities in Tallinn, October 2007.

28. Ibid.

29. Cory Welt, "Appendix 5: Russia and Its Post-Soviet Neighbors," in *Alternative Futures for Russia to 2017*, ed. Andrew C. Kuchins (Washington, DC: Center for Strategic and International Studies, 2007), 54–60.

30. Vladislav M. Zubok, *A Failed Empire: The Soviet Union in the Cold War from Stalin to Gorbachev* (Durham: University of North Carolina Press, 2009); "Foreign Minister Sergey Lavrov's Interview with Swedish Newspaper *Dagens Nyheter*, Moscow," April 28, 2016,

http://www.mid.ru/foreign_policy/news/-/asset_publisher/cKNonkJE02Bw/content/id/2258885?p_p_id=101_INSTANCE_cKNonkJE02Bw&_101_INSTANCE_cKNonkJE02Bw_languageId=en_GB; and Thomas T. Hammond, *Anatomy of Communist Takeovers* (New Haven, CT: Yale University Press, 1975).

31. Hanna Shelest, "Hybrid War & the Eastern Partnership: Waiting for a Correlation," *Turkish Policy Quarterly* 14, no. 3 (Fall 2015): 46, www.turkishpolicy.com/article/772/hybrid-war-the-eastern-partnership-waiting-for-a-correlation.

32. "Looking West—Estonian Minister of Defense Jaak Aaviksoo," *Jane's Intelligence Review*, October 2007.

33. John Arquilla, "The End of War as We Knew It? Insurgency, Counterinsurgency, and Lessons from the Forgotten History of Early Terror Networks," *Third World Quarterly* 28, no. 2 (2007): 382.

34. Conversations with Estonian authorities in Tallinn, October 2007.

35. Ibid.; Janusz Bugajski, *Cold Peace: Russia's New Imperialism* (Washington, DC: Center for Strategic and International Studies, Praeger, 2004); Richard Krickus, *Iron Troikas: The New Threat from the East* (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, 2006); and Keith C. Smith, *Russian Energy Politics in the Baltics, Poland, and the Ukraine: A New Stealth Imperialism?* (Washington, DC: Center for Strategic and International Studies, 2004).

Magdalena Rubaj and Tomasz Pompowski, "What Is the KGB Interested In?," *Fakt*, Warsaw (in Polish), October 19, 2004, in Open Source Center, FBIS-SOV, October 19, 2004; Jan Pinski and Krzystof Trebski, "The Oil Mafia Fights for Power," *Wprost*, Warsaw (in Polish), October 24, 2004, in FBIS-SOV, October 24, 2004; *Polish Radio 3*, Warsaw (in Polish), October 15, 2004, in FBIS-SOV, October 15, 2004; *PAP*, Warsaw (in Polish), December 13, 2004, in FBIS-SOV, December 13, 2004; and Open Source Center Analysis, "Lithuania: Businessman Stonys Wields Power with Russian Backing," FBIS-SOV, October 1, 2007.

36. Bugajski, *Cold Peace*; Krickus, *Iron Troikas*; and Smith, *Russian Energy Politics*. In Central Asia, when the Kyrgyz government backed away from ordering the United States to depart its military base there, Russia also simultaneously employed its economic power by rescinding its earlier loan to Kyrgyzstan and by revoking the preferred customs duties that Kyrgyzstan had been receiving on Russian diesel and energy imports, thus raising energy tariffs on its products. These moves forced the Kyrgyz government to announce major price rises in electricity fees that were the catalyst for the demonstrations that unseated President Kurmanbek Bakiyev. Just weeks before those demonstrations, the Russian press launched a media offensive denouncing Bakiyev as corrupt and saying that Russia could not work with him as if to signal that the time had come for an uprising. All these moves suggest a concerted plan to undermine the Bakiyev government and replace it with one more amenable to and openly dependent on Moscow. Although Putin professed surprise at the demonstrations, Russian papers discussed the possibility for demonstrations in Kyrgyzstan several weeks before the actual demonstrations occurred. Stephen Blank, "Moscow's Fingerprints in Kyrgyzstan's Storm," *Central Asia Caucasus Analyst*, April 14, 2010.

37. Eli Jellenc and Kimberly Zenz, *Global Threat Research Report: Russia*, iDefense Security Report, January 2007, cited in Kara Flook, "Russia and the Cyber Threat," Critical Threats, May 13, 2009, n6, http://www.criticalthreats.org/russia/russia-and-cyber-threat.

38. Ibid.

39. Richard Weitz, "Global Insights: Russia Refines Cyber Warfare Strategies," *World Politics Review*, August 25, 2009, www.worldpoliticsreview.com/articles/4218/global-insights-russia—refines-cyber-warfare-strategies.

40. Capt. Paulo Shakarian (USA), "The 2008 Russian Cyber Campaign against Georgia," *Military Review*, November–December 2011, 65.

41. Alexander Melikishvili, "The Cyber Dimension of Russia's Attack on Georgia," *Eurasia Daily Monitor*, December 12, 2008.

42. Ibid.

43. US Cyber Consequences Unit (CCU), "Overview by the US-CCU of the Cyber Campaign against Georgia in August of 2008," 2009, http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf.

44. Brian Krebs, "Report: Russian Hacker Forums Fueled Georgia Cyber Attacks," *Washington Post*, October 18, 2008, http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html.

45. US Cyber Consequences Unit, "Overview."

46. Ibid.

47. Melikishvili, "Cyber Dimension"; and David Hollis, "Cyberwar Case Study: Georgia 2008," *Small Wars Journal*, January 6, 2011, www.smallwarsjournal.com/jrnl/art/cyberwar-case-study-georgia-2008.

48. Ibid.; and US Cyber Consequences Unit, "Overview."

49. See Denis Volkov, "Supporting a War That Isn't: Russian Public Opinion and the Ukraine Conflict," Commentary (Washington, DC: Carnegie Endowment for International Peace, September 9, 2015), http://carnegieendowment.org/2015/09/09/supporting-war-that-isn-t-russian-public-opinion-and-ukraine-conflict/ih3x.

50. "Information Warfare," Levada Center, November 12, 2014, http://www.levada.ru/eng/information-warfare. Note: The link comes up with a warning.

51. George Gao, "Key Findings from Our Poll on the Russia-Ukraine Conflict: NATO Countries Blame Russia and Ukraine; Russians Blame West," Pew Research Center, June 9, 2015, http://www.pewresearch.org/fact-tank/2015/06/10/key-findings-from-our-poll-on-the-russia-ukraine-conflict/ft_15-06-09-nato-ukraine-russia/.

52. Geers, *Cyber War in Perspective*.

53. Ibid.

54. For more details, see Dina Evans, "Operation Armageddon: Cyber Espionage as a Strategic Component of Russian Modern Warfare" (Arlington, VA: Looking Glass, April 28, 2015), https://lgscout.com/press-release/lookingglass-cyber-threat-intelligence-group-links-russia-to-cyber-espionage-campaign-targeting-ukrainian-government-and-military-officials/.

55. "'Cyber Berkut' Hackers Target Major Ukrainian Bank," *Moscow Times*, July 4, 2014, http://www.themoscowtimes.com/business/article/cyber-berkut-hackers-target-major-ukrainian-bank/502992.html; "Pro-Russian Hackers Mug Key Ukrainian Bank," Nextgov, July 4, 2014, http://www.nextgov.com/cybersecurity/threatwatch/2014/07/stolen-credentials-network-intrusion-data-dump-pro/1225/; and Bill Gertz, "Russian Cyber Warfare Suspected in Bank Attacks," Flash/Critic, August 30, 2014, http://flashcritic.com/russian-cyber-warfare-suspected-bank-attacks-sophisticated-hackers/.

56. "Cyberberkut Hacked the Site of Ukrainian Ministry of Finance: The Country Has No Money," South Front, May 25, 2015, https://southfront.org/cyberberkut-hacked-the-site-of-ukrainian-ministry-of-finance-the-country-has-no-money/.

57. US Department of Homeland Security, "NCCIC/ICS-CERT Incident Alert: IR-Alert-H-16-043-01AP Cyber-Attack against Ukrainian Critical Infrastructure—Update A," March 7, 2016, 3, http://neih.gov.hu/sites/default/files/dlc/IR-ALERT-H-16-043-01AP.pdf.

58. Ivan Nechepurenko and Neil MacFarquhar, "As Sabotage Blacks Out Crimea, Tatars Prevent Repairs," *New York Times*, November 23, 2015, http://www.nytimes.com/2015/11/24/world/europe/crimea-tatar-power-lines-ukraine.html.

59. Ivan Nechepurenko, "Electricity Restored to Crimea after 2 Weeks of Darkness," *New York Times*, December 8, 2015, http://www.nytimes.com/2015/12/09/world/europe/electricity-restored-to-crimea-after-2-weeks-of-darkness.html.

60. *Natsional'naya Strategiya Bezopasnosti Rossii,* December 31, 2015.

61. Arquilla, "End of War," 383.