What's Next for Putin in Ukraine: Cyber Escalation?

by
Jason Healey
and
Michelle Cantos

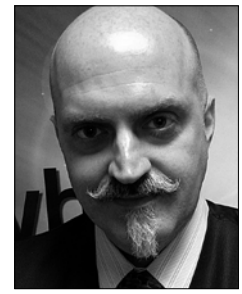
Chapter 17 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

In Chapter 17, Jason Healey and Michelle Cantos of Columbia University imagine four potential cyber conflict scenarios in this crisis. First, even if the hot war cools off, Russia can still raise the temperature in cyberspace, and cause serious network disruptions in Ukraine. Second, Russia could selectively target the West, adding a new vector to its already increased volume of threats, military exercises, submarine deployments, and nuclear warnings. Third, Vladimir Putin could mirror the 'frozen conflict' dynamic in cyberspace by threatening prolonged disruptions of the global Internet. And fourth, if the Ukraine conflict spins out of control, Russia, in desperation, might even have the power to take down the Internet entirely.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

What's Next for Putin in Ukraine: Cyber Escalation?



Jason Healey
Michelle Cantos
Columbia University

1 Introduction

We may be facing the internet's most dangerous moment.

From the earliest days of cyber intelligence, a rule of thumb was that 'those with the capability to cause significant cyber disruption lack the intent; those with the intent lack the capability'.[1] Some governments, including the United States, Russia, and China, have always had the capability, but have lacked the motivation to bring down the internet. However, times change, and Vladimir Putin, now facing strong sanctions and a weak rouble, could choose to retaliate against the West in the form of 'little green bytes'. US and European economies may, in fact, be natural targets, carrying the implicit message: if you seriously affect Russia's financial health, you too will feel the pain.

We may be facing the internet's most dangerous moment.

1 Matthew Devost. 'Risk of cyber terrorism raised at seminar,' *Massey University News*, September 12, 2002, http://www.massey.ac.nz/~wwpubafs/2002/news_release/13_09_02a.html.

Conflict in cyberspace offers adversaries many possibilities and Putin has numerous options. In the near term, there are four obvious scenarios: local instability, intimidation, frozen cyber conflict, and coercion.

The first option, local instability, would exclusively target Ukraine, causing cyber disruption in the hope of keeping the country prostrate while trying to avoid escalation with the West and a tightening of sanctions. In the second option, intimidation, Putin would use cyber capabilities against the West to mirror his existing recipe of strategic threats, military exercises, submarine deployments, nuclear threats and nuclear-capable bomber flights. A further escalation here could be a third option – a frozen cyber conflict, where techniques of hybrid warfare are used to try for medium-term disruption to the internet itself. The fourth option, coercion, would go beyond local disruption and provocations and would attempt to use cyber force to disrupt Western economic and military targets. This last scenario is the most dangerous of all, potentially signifying a calculation by Putin that Russia has little remaining stake in the global economic game. In that case, why not upend the table and ruin the party for everyone?

2 Local Instability: Frozen Conflict with a Topping of Cyber

In the least aggressive scenario, Putin would escalate only within Ukraine in an attempt to further destabilise and delegitimise the existing government. The 'little green bytes' might deny service to Ukrainian government and media sites, or even target critical infrastructure. As in other post-Soviet frozen conflicts, the goal is not necessarily to prevail, but rather to keep Ukraine destabilised for years and unable to pose any challenge.

As noted elsewhere in this book, the Russians, due to their legacy from the Moscow-dominated Soviet Union, have an extensive knowledge of Ukrainian systems. Most of Ukraine's infrastructure is well understood – if not designed by – Russian enterprises, so exploiting them for cyber attack would be far easier than for a typical cyber campaign elsewhere. There may also be a sufficient number of insiders who are friendly to Russia, and who could either be bribed or blackmailed into leaking sensitive government materials, disseminating propaganda, installing malicious software, or even physically destroying key systems.

Russia has shown some of its digital arsenal. Cyber espionage campaigns such as 'Sandworm' have played a role in intelligence collection operations against the Ukrainian government and some NATO nations, even taking advantage of multiple zero-day exploits.[2]

The local instability cyber option could allow Putin to maintain pressure on Ukraine while avoiding an increase in tensions with the West. He might even be

2 'iSIGHT discovers zero-day vulnerability CVE-2014-4114 used in Russian cyber-espionage campaign,' *iSight*, October 14, 2014, http://www.isightpartners.com/2014/10/cve-2014-4114/.

able to accomplish this while claiming to be de-escalating the conflict. Russia, in this scenario, would only launch disruptive cyber attacks *within* Ukraine, not against other targets in the West, and attempting to limit the upper bound of escalation. The international community might be happy, however, to countenance a 'cyber war' in Ukraine if it caused little tangible damage to other countries, limited the body count, and generated fewer disturbing media images.

3 Intimidation: Cyber Provocations and Escalation

A second option for Putin is to send a digital warning shot across the West's cyber bow, in effect saying that Russia has additional cards up its sleeve and may play them if necessary. Russia is already escalating all sorts of military operations against the West, from massive exercises and military flights to nuclear threats. 'Little green bytes' could therefore be just one additional form of provocation to add instability on the world stage.

Such attacks would be just-deniable-enough and might target defence and military systems and networks. Russia could target allies with weaker defences, or governments which Putin might calculate as being easier political prey, and more susceptible to Russian coercion.

This cyber escalation would simply be a natural extension of Putin's provocative behaviour in other military forces. In the last fifteen months, Russia has apparently sneaked submarines into Swedish and Finnish territorial waters, stating that Finland's growing ties with NATO were a 'special concern';[3] flown jet fighters and nuclear-capable bombers along the periphery of Europe; and buzzed NATO ships including the US guided-missile destroyer USS Ross as it sailed in international waters off the Russian-occupied Crimean peninsula.[4]

Apart from drilling his conventional forces, Putin in the spring of 2014 organised large-scale exercises designed to assess the preparedness level of his nuclear forces.[5] In the context of Russia's nuclear threats against Denmark, these appear to be calculated (if clumsy) efforts to intimidate the West.[6]

The Russian cyber assault on Estonia in 2007 was a blueprint for a geopolitically inspired and just-deniable-enough digital disruption. When

Estonia in 2007 was a blueprint for a geopolitically inspired and just-deniable-enough digital disruption.

3 'Finnish military fires depth charges at suspected submarine,' *Reuters*, April 28, 2015, http://www.reuters.com/article/2015/04/28/us-finland-navy-idUSKBN0NJ0Y120150428.

4 Barbara Starr. 'Russian planes, U.S. warship have close encounter near Crimea,' *CNN*, June 1, 2015, http://www.cnn.com/2015/06/01/politics/russia-plane-navy-uss-ross/.

5 Bill Gertz. 'Russia Conducts Large-Scale Nuclear Attack Exercise,' *Washington Free Beacon*, May 8, 2014, http://freebeacon.com/national-security/russia-conducts-large-scale-nuclear-attack-exercise/.

6 Adam Withnall. 'Russia threatens Denmark with nuclear weapons if it tries to join NATO defence shield,' *The Independent*, March 22, 2015, http://www.independent.co.uk/news/world/europe/russia-threatens-denmark-with-nuclear-weapons-if-it-tries-to-join-nato-defence-shield-10125529.html.

the Estonian government decided to move a Soviet war memorial from the centre of its capital Tallinn to a military cemetery on the outskirts of town, Russia responded by encouraging 'patriotic hackers' to engage in a three week long Distributed Denial-Of-Service (DDoS) attack against numerous sectors of the Estonian economy including the government, media, and financial institutions.[7] This template relies on a combination of threats, cyber capabilities, the use of proxies, and plausible deniability.

Russia might alternately hold off on such disruptive attacks in favour of increasingly aggressive espionage. In fact, it seems an escalation in such intrusions is already underway.

Russian state-sponsored hackers are believed to have recently compromised the US Department of State, then used that access to penetrate the unclassified network of the Executive Office of the President.[8,9] Unlike during previous intrusions linked to Russia, on this occasion the digital spies did not back out of the system once they were discovered, but fought back in order to maintain their foothold in the network.[10] Investigators also believe that Russian spies were behind the recent intrusion into the unclassified email of the Joint Chiefs of Staff, an intrusion which forced the Pentagon to take the system down for several days.[11]

4 Freezing the Conflict in Cyberspace

Rather than, or in addition to, using cyber to help destabilise the Ukraine, Putin might try to make the internet itself a new zone of frozen conflict. This option is perhaps not as likely as the others, but might offer Putin an intriguing possibility: inflict on the internet, which delivers 'harmful' content in the form of unwanted truths to Russian citizens, just enough long-term disruption so that it is less useful, less trusted, and less an enabler to Western economies and societies.

In this option, Putin's forces would use cyber capabilities to periodically disrupt core internet infrastructure such as the domain name system, or frequently take down Western information providers. Each new week could see a large-scale denial-of-service attack.

This option differs from the previous 'intimidation' option in two ways. First, the attacks would be far more disruptive than mere shows of force. Compared to

7 Ian Traynor. 'Russia accused of unleashing cyberwar to disable Estonia,' *The Guardian*, May 16, 2007, http://www.theguardian.com/world/2007/may/17/topstories3.russia.

8 Evan Perez and Shimon Prokupecz. 'Sources: State Dept. hack the 'worst ever'," *CNN*, March 10, 2015, http://www.cnn.com/2015/03/10/politics/state-department-hack-worst-ever/index.html.

9 Ellen Nakashima. 'Hackers breach some White House computers,' *The Washington Post*, October 28, 2014, http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fa0-5ef7-11e4-91f7-5d89b5e8c251_story.html.

10 Michael S. Schmidt and David E. Sanger. 'Russian Hackers Read Obama's Unclassified Emails, Officials Say,' *New York Times*, April 25, 2015, http://www.nytimes.com/2015/04/26/us/russian-hackers-read-obamas-unclassified-emails-officials-say.html

11 Nancy A. Youssef. 'Russians Hacked Joint Chiefs of Staff,' *The Daily Beast*, August 6, 2015, http://www.thedailybeast.com/cheats/2015/08/06/russians-hacked-joint-chiefs-of-staff.html.

the intimidation option where Russia threatens force to avoid a conflict, in this frozen-conflict option, Putin already accepts Western nations as adversaries. The goal is therefore not to get them to back down, but hopefully to destabilise the internet just enough to deny cyber benefits to his perceived enemies.

5 Coercion: Escalate to De-escalate

What if, Sony-style, one bank a week were targeted for a disruptive and embarrassing attack?

The most aggressive option for Putin is to use cyber capabilities to disrupt the economies of the West. Imagine a massive, long-term and continuing attack against the West's financial system or power grids. What if, Sony-style, one bank a week were to be targeted for a disruptive and embarrassing attack?

Russia in the past had, along with at least the United States and China, the capability to conduct such attacks, but lacked the intent. Russia had disagreements with the West but was not engaged in any real conflict. Further, to some extent, Russia needed healthy Western economies to itself thrive.

That situation has changed. Today, Putin may well see himself in a conflict with the West, perhaps even a shooting war, and feel the very survival of his regime could be at stake. In 2013, sanctions including asset freezes and export prohibitions pushed Russia to the brink of a recession, and the economy grew by only 1.3%.[12] By the end of 2015, the World Bank predicts that ongoing sanctions coupled with the decrease in oil prices will shrink the Russian economy by 3.8%.[13] Putin could calculate that Russia has few remaining stakes in the global economy and financial system.

Without international economic entanglement, it is far easier for Putin to use Russia's impressive cyber capabilities to try to directly coerce (rather than threaten) the West. By inflicting economic turmoil, he could turn Russia's lack of a stake in the global financial system from a liability into an asset. With nothing to lose and everything to gain, Putin might calculate that unleashing his just-deniable-enough 'little green bytes' against Western economies could be a win-win situation for Russia.

Russia is already pushing the idea that they may need to 'escalate to de-escalate' a brewing conflict with the West. In an extensive article in *Vox*, Max Fisher lays out the evidence that the world is ever closer to conflict, even a world war, and especially that Putin 'has enshrined, in Russia's official nuclear doctrine, a dangerous idea no Soviet leader ever adopted: that a nuclear war could be winnable'.[14]

12 'How far do EU-US sanctions on Russia go?' *BBC*, September 15, 2014, http://www.bbc.com/news/world-europe-28400218

13 Andrey Ostroukh. 'Russia's Economic Outlook Worse Than Thought, World Bank Says,' *The Wall Street Journal,* April 1, 2015, http://www.wsj.com/articles/russias-economic-outlook-worse-than-thought-world-bank-says-1427883522.

14 Max Fisher. 'How World War III Became Possible,' *Vox*, June 29, 2015, http://www.vox.com/2015/6/29/8845913/russia-war.

In that light, cyber weapons may offer an even more attractive opportunity given that cyber effects can be temporary and reversible. Russian Deputy Prime Minister Dmitry Rogozin has already declared that Russian tanks 'don't need visas' to cross international borders.[15] If Russia is willing to make nuclear threats and roll T-72s across borders, then how much more likely are attacks using faster, more deniable, electrons?

One obvious target would be Western financial firms that currently enforce the sanctions against Russia. Many analysts believe that Iran chose precisely this form of retaliation in 2012, in response to Stuxnet.[16] Other obvious targets could be the oil, gas, or electricity sectors, in order to raise the price of oil.

During our research for this chapter, several security analysts stated that Russia may be preparing for this contingency with its Havex and BlackEnergy cyber campaigns.[17] In both cases, Russian government hackers apparently targeted Western energy companies, not for espionage, but in order to prepare for a potential follow-on disruptive attack. It appears Russia has proved that it has the required capabilities already in place to disrupt Western energy systems, now it is just a matter of having the intent.

Or Putin could focus his cyber attack not against sectors, but against specific Western allies; those he felt would be most likely to submit to coercive pressure. His whispered promise might be something along the lines of 'Drop your support for sanctions and all these cyber failures you're experiencing can just go away.' Countries which might not have been fully committed to the sanctions in the first place might not need much convincing.

6 Conclusion

Cyberspace – and cyber attacks – offer many ways, especially for a capable nation-state, to target an adversary. In the current conflict, the most likely near-term options for Russia are perhaps local instability, intimidation and coercion. Of course, the scenarios discussed in this chapter are not mutually exclusive; Putin could jump between them or even employ them all simultaneously.

Fortunately to help analyse Russia's cyber current actions, it may be enough to analyse his actions in the physical world: Russian hostility in Europe is likely to be matched with Russian hostility online. If this process starts to get out of control, then Western leaders have to be at their highest level of concern.

If Putin believes he is approaching a use-it-or-lose-it situation for his autocratic regime and its stolen billions, he may just decide to take the internet down with him.

15 'Russian Official: 'Tanks Don't Need Visas', *Defense One/Agence France-Presse,* May 25, 2015, http://www.defensenews.com/story/defense/international/europe/2015/05/25/russian-official-tanks-need-visas/27924351/.

16 Siobhan Gorman and Julian Barnes. 'Iran Blamed for Cyberattacks,' *The Wall Street Journal*, October 12, 2012, http://www.wsj.com/articles/SB10000872396390444657804578052931555576700.

17 Blake Sobczak and Peter Behr. 'Secret meetings tackle back-to-back energy-sector cyberthreats,' *EnergyWire*, October 31, 2014, http://www.eenews.net/energywire/stories/1060008193.