‘Compelling Opponents to Our Will’: The Role of Cyber Warfare in Ukraine

by
James Andrew Lewis

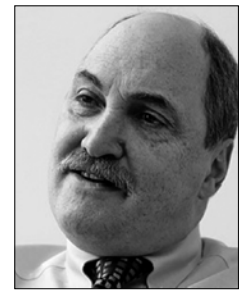
Chapter 4 in
Kenneth Geers (Ed.), Cyber War in Perspective:
Russian Aggression against Ukraine,
NATO CCD COE Publications, Tallinn 2015

CCDCOE
NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

James Andrew Lewis of the Centre for Strategic and International Studies (CSIS) analyses the geopolitical effects of cyber attacks in Chapter 4. He discusses two metrics: strategic effects that diminish an opponent's will or capacity to fight (e.g. influencing public opinion) and tactical effects that degrade military power (e.g. confusing troops, or denying service to weapons). Success is premised upon observable, real-world effects. In Ukraine, Russian cyber operations had no strategic effect and only a limited, short-term political effect.

NATO Cooperative Cyber Defence
Centre of Excellence Tallinn, Estonia

'Compelling Opponents to Our Will': The Role of Cyber Warfare in Ukraine



James Andrew Lewis

Centre for Strategic and International Studies (CSIS)

1 Metric for Cyber Attack

The conflict in Ukraine has challenged fundamental elements of Western alliance strategy. Russian efforts exploit a general reluctance by the West – natural in democracies – to risk war. The West has been unable to deter Russia from its adventure.

Cyber warfare has played only a limited role in this. The concepts of strategic and military effect provide us with two metrics for assessing the effect of cyber attacks generally, and for Russian cyber activities in Ukraine. Strategic effect would be to diminish the opponent's will or capacity to resist. This can include politically coercive cyber actions such as were used against Estonia. Military effect would be degradation in the performance of commanders, troops, and weapons, demonstrated by U.S. actions in its Middle Eastern conflicts or as part of the 2007 Israeli airstrike in Syria[1].

Cyber attacks that produce strategic or military effect can include the manipulation of software, data, knowledge, and opinion to degrade performance and produce political or psychological effect. Introducing uncertainty into the minds of opposing commanders or political leaders is a worthy military objective. Manipulating public opinion to damage an opponent's legitimacy and authority in both domestic and international audiences is also valuable. Some actions may provide only symbolic effect aimed at a domestic audience, but this too is valuable for a nation in conflict.

1 David Makovsky. 'The Silent Strike: How Israel bombed a Syrian nuclear installation and kept it secret,' *The New Yorker*, 17 September 2012, http://www.newyorker.com/magazine/2012/09/17/the-silent-strike.

To assess non-kinetic effect as a contributor for strategic or military advantage, we must look for observable effects in three categories: creating confusion, shaping opinion, and inflicting damage to data or services. Using these metrics, we can conclude that Russian cyber efforts in Ukraine produced an early tactical effect that has since tapered off and, since they are limited to actions that do not produce physical or disruptive consequences, have largely failed to achieve strategic or military effect.

2 Strategic and Military Effect

The Ukraine conflict has been described as hybrid warfare; a mixture of unconventional tactics and strategies, irregular forces, covert action, cyber operations, and political manipulation to achieve strategic goals. In essence, hybrid warfare is a collection of tactics designed to circumvent deterrence and avoid military retaliation by skirting the threshold of what could be considered state use of armed force. In this new style of conflict, non-kinetic actions can be as important as kinetic attacks. Hybrid warfare highlights the central problem for our understanding and management of interstate conflict; conventional warfare is now only part of a larger range of coercive actions available to nations.

Cyber operations – the ability to remotely manipulate computer networks – have created a capability that is well suited to this new political-military environment. Cyber capabilities create an operational space in which nations can conduct offensive action with less political risk, given the grey area in international law which cyber war inhabits, and where opponents can find it difficult to respond. Advanced cyber action can create physical effects equivalent to kinetic attack, but we should not interpret cyber capabilities solely from the perspective of physical effect.

> *Cyber capabilities create an operational space in which nations can conduct offensive action with less political risk.*

While cyber attacks can produce effects similar to kinetic weapons, there is an informational aspect involving the manipulation of opinion and decision-making that is equally important and much more frequently used. Cyber attack can produce results equivalent to kinetic attack, but this is not its primary effect, which (at least for now) is to manipulate data, knowledge, and opinion to produce political or psychological effect rather than physical damage. Introducing uncertainty into the minds of opposing commanders or political leaders is a worthwhile military goal, as it will cause them to make mistakes or to become hesitant, providing the attacker with dominance of the battle space and the advantage of putting the defender in a reactive posture. Cyber actions that manipulate public opinion to

affect an opponent's legitimacy and authority are also valuable in conflict among states.

Cyber attack creates an operational space for coercive action that avoids many of the political risks of kinetic warfare. Cyber attacks are attractive in that they offer varying degrees of covertness and their treatment under international law remains ambiguous in regard to whether they qualify as an 'armed attack' that would legitimise retaliation. Although cyber tools and techniques can be used in harmful ways, they are not weapons *per se*, which can make it difficult to decide when a cyber incident can be considered an armed attack or a use of force.

An initial effort to define how a cyber incident could qualify as a use of force or armed attack would be to consider that an effect of the cyber action was the equivalent of an attack using conventional weapons producing physical destruction or casualties. A cyber incident that produced injury or death to persons and the destruction of or damage to property would certainly be considered as a use of force or armed attack. A cyber attack that produced intangible effects of such scope, intensity, and duration that they are judged to have consequences or harmful effects of sufficient scale and gravity could also be considered an armed attack.

No Russian action in Ukraine rises to this level. Overall, the use of offensive cyber capabilities for kinetic effect has been minimal, with only a few known incidents. Russia is one of the most skilled among the nations who have developed cyber capabilities, but we have not seen extensive use of actual attacks against Ukraine. Neither critical infrastructure nor Ukrainian weapons have been damaged or disrupted. Russia has used its cyber capabilities primarily for political coercion, opinion-shaping, and intelligence gathering, and these cyber operations fall below the threshold set in Article V of the North Atlantic Treaty. Operations in Estonia, Georgia, and now Ukraine suggest that NATO may need to adjust its thinking about how opponents will use cyber attacks.

Russia has been relatively careful in the overt use of its own forces – especially compared to its actions against Georgia where the Russian Ministry of Defence confirmed that Russian armoured units were engaged in combat for 'peace enforcement'. The Russian army occupied Georgian territory and Russian aircraft bombed targets including the capital.[2] Russian actions in Ukraine took a different course. The current caution may reflect lessons learned in Georgia or a desire to preserve some degree of deniability, and manoeuvring to avoid an overt violation of international law.

Cyber attack does not require 'an act of violence to compel our opponent to fulfil our will'.[3] Violence through cyber means is possible, but that is not the only or even primary use of cyber attack. Its effects are more often intangible and

2 Library of Congress, *Russian Federation: Legal Aspects of War in Georgia*, http://www.loc.gov/law/help/russian-georgia-war.php.

3 Clausewitz's definition of war.

informational, and are intended to manipulate data, create uncertainty, and shape opinion. An emphasis on kinetic effect can obscure important operational distinctions in the use of cyber techniques and complicates efforts to develop norms for cyber conflict.

3 Norms and the Application of International Law[4]

Russia's activities in Ukraine have implications for both cyber warfare and for cyber norms. Russian actions have carved new contours for conflict that do not map perfectly to existing concepts and rules for warfare and defence. Existing norms and laws for armed attack were based on the use or threat of use of physical violence and force. These must be adjusted, if not amended, for cyber conflict.

Efforts to redefine violence and force to include the full range of possible cyber actions (such as Russian and Chinese efforts in the United Nations (UN) to define information as a weapon[5]) have so far introduced more ambiguity than clarity. Information is clearly not a weapon, but a minimalist definition that emphasises kinetic effect is also inadequate in capturing the full range of cyber effects.

> *The 'rules' for cyber conflict pose a challenge to existing international law.*

As such, the 'rules' for cyber conflict pose a challenge to existing international law. Currently, there is no agreement among leading nations, and it is interesting to note that with the 2015 Group of Governmental Experts (GGE), which was tasked to look at the application of international law to cyber conflict,[6] this topic proved to be the most difficult. Disagreements over the application of international law between Russia, China and a few others on one hand, and NATO nations on the other, almost derailed the talks.

The crux of the disagreement was over the application of specific provisions of the UN Charter, (the general applicability of the Charter had been agreed to in earlier GGEs), and in particular the applicability of Article 2/4 (renouncing the use of force) and Article 51 (the inherent right to self-defence). One question for the development of further norms for cyber conflict becomes whether it is possible to move beyond the norms embedded in the UN Charter and the international agreements governing the conduct of warfare and armed conflict, to address this new aspect of warfare and to create norms that govern non-ki-

4 The author was rapporteur to the UN Group of Governmental Experts in 2010, 2013 and 2015.

5 See, for example, SCO, *Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security*, 2009, https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf [in Russian].

6 Along with norms and confidence building measures, see *Group of Governmental Experts Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174, 22 July 2015, UNODA, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

netic action. One possible avenue for progress would be to expand the Charter commitment to avoid actions that threaten the territorial integrity or political independence of a state (found in Articles 2/4 and 51) to explicitly include cyber actions.

Continued ambiguity over the application of these UN Charter articles serves the interests of Russia and China by not creating grounds for or legitimising retaliation for cyber actions.[7] This includes a general rejection of Western efforts to define 'use of force' and 'armed attack' using the concepts of equivalence and effect. These ambiguities, however, are not unique to cyber conflict, date from the signing of the Charter, and reflect conflicting desires to renounce the use of force while preserving the right to use force in self-defence. The Russian and Chinese goal, similar to other actions in arms control negotiations by these countries, is to constrain the U.S. and its allies.

Intentional ambiguity may define the emerging strategic conflict between Russia and the West for the foreseeable future. Russian cyber tactics accentuate and expand ambiguity. The Russian concept of cyber warfare blends elements of what would be considered information warfare in the West. It is well known that the Russians prefer to use the phrase 'information conflict' to 'cyber conflict' on the grounds that cyber is too narrow and technical. Unsurprisingly, this preference reflects their use and understanding of cyber techniques.

The norms before the UN General Assembly for approval at its 70th session will reiterate the rule of international law and the UN Charter, although how these are to be applied is a matter of intense dispute. They call for states not to attack critical infrastructure in peacetime, and to take note of the principles of humanity, necessity, proportionality, and distinction whey they exercise their inherent rights recognised by the UN Charter, including the right of self-defence. They do not address the use of cyber tools for political coercion, and it is interesting and indicative to note that Russia, which has made the most frequent use of cyber coercion, is the leading proponent for such norms.

State practice suggests that there is an implicit threshold among states to avoid cyber actions against each other that could be interpreted as the use of force or an armed attack. This creates implicit norms for state behaviour derived from international practice that constrain malicious cyber actions, but these implicit norms are inadequate for this new form of conflict. The kind of cyber conflict we have seen in Ukraine poses a challenge not only to existing Western strategy (which is based on international law and UN Charter commitments) but also for the development of norms. If the trend in warfare is to circumvent direct confrontation between conventional forces (particularly the conventional forces of the U.S. and its allies), and if cyber conflict will often not involve kinetic effect or territorial intrusions, existing norms and rules for conflict will have limited application.

7 According to conversations between the author and GGE representatives from many countries.

We can place cyber norms into four categories:

- Those that call for observation of existing international law regarding state responsibility, especially the laws of armed conflict;
- Those that seek to exempt from cyber attack infrastructures where an attack could have an indiscriminate effect such as critical infrastructures, including the infrastructure of the global internet;
- Norms on state responsibilities to assist other states that are the victim of cyber attacks; and
- Norms on the proliferation of cyber technologies that could be used for malevolent purposes (which is still nascent and suffers from definitional problems).

None of these norms can be easily extended to the new modes of coercion created by cyber capabilities. The stricture that comes closest is the Article 2/4 commitment to refrain from the use of force against the political independence of another state, but cyber actions such as we have seen in Ukraine cannot be considered a use of force.

Cyber actions that do not have physical effect and which are taken outside the context of formal conflict do not fit well with the existing structure of international practice. Nations appear to observe an implicit threshold for their use of cyber tools and with very few exceptions, have avoided actions that could be considered under international law as a use of force or an armed attack. Attempts to expand these implicit understandings or to redefine the use of force to include coercive or politically manipulative cyber actions immediately run into problems. The central problem is access to information, because several countries would happily support a norm that restricts access to information.

> *Nations appear to observe an implicit threshold for their use of cyber tools.*

Russia, in particular, is quick to label any criticism of its behaviour as disinformation, information warfare, or propaganda. Russian negotiating behaviour, shaped in good measure by Soviet precedent, is often defensive, seeking to constrain the U.S. and its allies in areas where the West has a technological advantage, or to limit the political risks the internet creates. This defensive orientation creates a negotiating agenda that conflicts with Western countries when it comes to norms.

4 Comparing Ukraine to Estonia and Georgia

Contrasting Russian cyber activities in Ukraine with Estonia and Georgia is helpful in assessing their use and value, as well as in considering what new norms might look like. The cyber attacks in Estonia[8], composed of service disruptions and denial

8 Eneken Tikk, Kadri Kaska and Liis Vihul. *International Cyber Incidents: Legal Considerations* (Tallinn, Estonia: NATO Cooperative Cyber Defence of Excellence, 2010).

of service incidents, could best be compared to the online equivalent of a noisy protest in front of government buildings and banks. They had little tangible effect, but they created uncertainty and fear among Estonian leaders as they were considered a potential precursor to armed Russian intervention. In Georgia[9], cyber attacks were closely coordinated with Russian military operations.

The effects of the cyber attacks in Estonia and Georgia deserve more careful study. The attacks did not cripple or bring Estonia to its knees, and NATO's decision not to invoke Article V reflects this fact. They were frightening not because of the cyber effect, but because of Estonian concerns about Russian intentions, NATO's reliability, and their internal Russian-speaking minority. Similarly, cyber attacks on Georgia were largely symbolic. The most visible incident was the defacement of the Georgian President's website by Russian hackers, who drew moustaches on his photograph. The most interesting part of the Georgia episode was the close operational coordination between the hackers and the Russian military. The Russians continue to experiment with cyber tools to support their political objectives.

If the Russian goal in Ukraine is to shape global public opinion, there were some early successes in painting the Ukrainians as 'fascists' (a favoured communist insult) guilty of human rights violations. But no one believes that anymore, and the tide of public opinion has turned heavily against Russia. A recent Pew Research survey on global opinion captures the change and is entitled 'Russia, Putin, Held in Low Esteem around the World'.[10] In this, the current Russian regime has not done as well as its communist predecessors, who could at least cloak their actions in the rhetoric of Marxism. Russia's current effort to hire hundreds of internet trolls[11] to insert pro-Russian opinions in the Western press has proven to be feckless. Perhaps the benefit is domestic, persuading the Russian population of the righteousness of Russia's course of action,[12] but as a tool of coercion, the absence of informational disruption (as in the case of Sony or Aramco) or physical effects (as with Stuxnet) makes Russian cyber operations annoying, but ultimately inconsequential.

If the Russian goal is to shape global public opinion, there were early successes in painting the Ukrainians as 'fascists'.

The most successful Russian tactics were creating or supporting pro-Russian separatist groups in areas with significant Russian-speaking minorities and then using Russian special and ultimately conventional forces to stiffen and protect these groups from the Ukrainian response. Cyber attack was largely irrelevant.

9 *Ibid*.

10 Bruce Stokes. 'Russia, Putin, Held in Low Esteem around the World,' *Pew Research Centre*, 5 August 2015, http://www.pewglobal.org/2015/08/05/russia-putin-held-in-low-regard-around-the-world/.

11 See, for example, Dmitry Volchek and Daisy Sindelar, 'One Professional Russian Troll Tells All,' *RadioFreeEurope/RadioLiberty*, 25 March 2015, sec. Russia, http://www.rferl.org/content/how-to-guide-russian-trolling-trolls/26919999.html.

12 Katie Simmons, Bruce Strokes and Jacob Poushter. 'NATO Publics Blame Russia for Ukrainian Crisis, but Reluctant to Provide Military Aid,' *Pew Research Centre*, 15 July 2015, http://www.pewglobal.org/2015/06/10/2-russian-public-opinion-putin-praised-west-panned/.

Both Western and Russian analysts may have drawn the wrong lessons from Estonia and Georgia. States (especially states with a fondness for Lenin) will use cyber attacks for politically coercive purposes and might use them for military purposes, to disrupt data or services. But the incidents in Ukraine did not disrupt command and control, deny access to information, or have any noticeable military effect.

This means that we (and the Russians) may overestimate the coercive effect of cyber attacks and that their real military value is achieved when there is physical effect or disruption of data and critical services, something that most denial of service attacks cannot produce. Cyber attacks are a support weapon and will shape the battlefield, but by themselves they will not produce victory. Cyber attacks support other weapons and operations, as in the 2007 Israeli attack against Syrian air defence. This is still a subject of intense debate, but experience suggests that it is easy to exaggerate the effect of cyber attack. A more accurate assessment would rank cyber activities into three categories: espionage, operational, and political. However, note that the benefits of the former are clear, while the latter are open to question.

To provide strategic or military effect, cyber actions must produce destructive effect and be integrated into existing military structures, doctrine, planning, and operations. Estonia and Georgia can be contrasted with two known attacks that did have military effect. The Israeli air strike against a Syrian nuclear facility is reported to have used cyber means to disrupt Syrian air defence radars, allowing the aircraft to fly undetected across much of the country.[13] In this case, there was no physical damage but a vital service was disrupted. With Stuxnet, there was physical damage, albeit inflicted covertly, that could be duplicated in overt warfare, noting that a degree of caution is warranted to predict the effect of cyber attacks on civilian infrastructure.[14] We should also note the reported use of cyber techniques by the U.S. to disrupt or confuse Taliban command and control, often with lethal results for the insurgents.[15] If cyber is the weaponisation of signals intelligence, it appears that to have actual military effect, there must be physical damage.

> *If cyber is the weaponisation of signals intelligence, there must be physical damage.*

This is a consideration of cyber as a tool of military action and does not consider either traditional methods of electronic warfare, which Russia has used extensively in Ukraine,[16] nor the intelligence value of Russian cyber espionage. We do not know the role cyber espionage played in these efforts, but if Russian successes against the United States are any guide, we can assume cyber spying made a positive contribu-

13 David Makovsky. 'The Silent Strike: How Israel bombed a Syrian nuclear installation and kept it secret,' *The New Yorker*, 17 September 2012, http://www.newyorker.com/magazine/2012/09/17/the-silent-strike.

14 Kim Zetter. 'An Unprecedented Look At Stuxnet, The World's First Digital Weapon,' *Wired*, 3 November 2014, http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

15 Interviews with US military officials.

16 Joe Gould. 'Electronic Warfare: What US Army Can Learn From Ukraine,' *Defense News*, 4 August 2015, http://www.defensenews.com/story/defense/policy-budget/warfare/2015/08/02/us-army-ukraine-russia-electronic-warfare/30913397/.

tion. That Russia has completely penetrated Ukrainian communication networks and has unparalleled access to Ukrainian communications is likely to provide considerable value for Russian tactics and planning, but cyber as a tool of coercion has proven to be of limited utility.

This is certainly not the cyber war as it is often depicted in public media, but it does not mean that cyber attack is overrated and militaries can deemphasise it. That would be a rash conclusion. It means that the Russians, for whatever reason, chose not to use the most damaging forms of cyber attack against Ukraine, Georgia, or Estonia. If allegations that Russia were responsible for damaging cyber attacks on a German steel mill[17] and a Turkish pipeline[18] are correct, these would demonstrate that Russia has the capability necessary for cyber attacks that would create physical damage and qualify as a use of force. Russia's 2008 exploit in penetrating Central Command's classified networks[19] was an early demonstration of its ability to implant malware on an opponent's networks that could erase data and disrupt command and control, but the Russians chose not to do this.

In Ukraine, Russia has experimented with how best to produce military and political benefits from cyber operations. Political context and alliance relationships have a powerful influence in constraining the use of force, including cyber attacks. Its cyber actions appear to reflect a decision not to engage the full range of Russian cyber capabilities. Other potential opponents, including NATO, should not assume that in the event of conflict, the Russians will make the same decision.

17 'Hack attack causes 'massive damage' at steel works,' *BBC*, 22 December 2014, http://www.bbc.com/news/technology-30575104.

18 Ariel Bogle. 'A Cyber Attack May Have Caused a Turkish Oil Pipeline to Catch Fire in 2008,' *Slate*, 11 December 2014, http://www.slate.com/blogs/future_tense/2014/12/11/bloomberg_reports_a_cyber_attack_may_have_made_a_turkish_oil_pipeline_catch.html.

19 Phil Stewart and Jim Wolf. 'Old worm won't die after 2008 attack on military,' *Reuters*, 16 June 2011, http://www.reuters.com/article/2011/06/17/us-usa-cybersecurity-worm-idUSTRE75F5TB20110617.