The Impact of Cyberattacks on Civil Wars Examining Russia's Role in the Ukrainian Conflict

PARIS MARX, *Memorial University of Newfoundland*

Abstract. Cyberattacks are a relatively new tool to be used in civil wars, and the understanding of their impact remains in the preliminary stages. This paper reviews the existing literature on the impact of cyberattacks on civil wars, identifying particularly how they are difficult to attribute to a particular state or non-state group. It then applies that understanding to the ongoing conflict in Ukraine, where cyberattacks have been used by Russia and its proxies to aid pro-Russian separatist groups.

Introduction

Civil wars are devastating and complex events that researchers are still trying to fully understand. The wide range of factors that must be considered make it difficult to create a single generalizable theory that can be applied to every country or region of the world, and the task only becomes more difficult with the impact of new technologies on such conflicts.

Cyberattacks are among these new technologically enabled mechanisms that are increasingly being utilized in civil wars, yet because they have only been used in the past couple of decades, and there is a disparity between when events occur and the time it takes for researchers to understand them and publish their findings, the literature on the impacts of cyberattacks on civil wars remains at an early stage. That does not, however, mean that there are not trends that can be observed in the studies that have been undertaken.

In conflicts where one or both of the parties have used cyberattacks, it has been difficult to attribute them to a particular group or even a specific location. These attacks have given aggressors a means to attack their enemy through cyberspace instead of with a physical presence, they have increased confusion and mental distress for citizens, and they have encouraged states to work more closely with non-state actors to cultivate plausible deniability. Another trend that emerged in the literature was the prominent role played by Russia in pioneering many of the techniques surrounding cyberattacks, and, importantly, how they hold a more expansive view of what constitutes cyberwarfare as opposed to the conception popularized by Western states.

It is very clear that each of these developments could have significant impacts on the duration, lethality, and dynamics of civil wars, making the study of the impact of cyberattacks on civil wars not only timely, but also essential. The prevalence of cyberattacks will not lessen in the future, but instead, will only increase in their frequency and scope as both state and non-state actors improve their cyberwarfare capabilities, and as new countries and groups develop the skills to undertake these attacks. This presents many issues, but potentially the most significant is the difficulty of attributing the attack to any one perpetrator, especially if they happen to be a proxy of a large and powerful state.

In order to demonstrate the growing impact of cyberattacks on civil wars and the difficulties that they present, I will begin this paper by reviewing the existing literature both on cyberattacks and the role that Russia has played in this new era of warfare. I will then apply this knowledge to the case study of the seizure of Crimea by Russia and the ongoing civil war in Ukraine, where there is a strong Russian influence both in supporting the pro-Russian separatists and in using cyberattacks against the Ukrainian government. Since Russia has been one of the leaders and innovators in the use of these tactics, this is an instructive case that will provide lessons that can be applied in the study of future events.

Literature Review

Before getting into a broader discussion of the literature on cyberattacks, it would be helpful to get a foundational idea of what they are. Gandhi et al. present a broad definition of cyberattacks as "any act by an insider or outsider that compromises the security expectations of an individual, organization, or nation" (2011: 29). These attacks take place in cyberspace, which is "a massive sociotechnical system of systems," of which humans remain a major component, and instead of simply being random acts, evidence increasingly indicates that they occur in conjunction with social, political, economic, and cultural conflicts (Gandhi et al., 2011: 29). While cyberattacks as a form of protest are taken as a reaction to an event, they have also been observed to take place in advance of, or during military conflicts (Gandhi et al., 2011: 35).

There are several types of cyberattacks that can be undertaken. Denial-of-service (DoS) attacks are the most basic, consisting of either the defacing of websites, or rendering them unavailable for a period of time. Network-exploitation attacks, result in data theft or the planting of hidden files that are difficult to locate and can take down a whole computer network when activated (Klimburg, 2011: 42-43). DoS attacks can also cause psychological impacts, including fear among the population when online services become inaccessible (Gandhi et al., 2011: 37). Potentially more damaging attacks can also be conducted on key pieces of infrastructure, including banks, energy grids, and transportation systems; and, if they cause "substantial human and/or material destruction", they could be considered an armed attack, which could warrant retaliation (Gandhi et al., 2011: 37; Tsagourias, 2012: 230-31).

However, whereas the Western view of cyberattacks is generally confined to the security compromise that takes place in cyberspace, Russia has a notably broader interpretation. Erol and Oguz call it "hybrid warfare," encompassing a blurring of the borders between different types of warfare, thus combining cyberattacks and disinformation campaigns to confuse the targeted state and taking advantage of this confusion through the use of disguised military operations. (2015: 264-67). Giles observes a similar phenomenon of Russian "information war," which comprises cyberattacks along with "electronic warfare, psychological operations, strategic communications and influence," and, most importantly, these actions are constant, taking place both in times of peace and of war (2011: 46-48).

Due to the nature of cyberspace, much of the literature concurs that it is difficult to attribute cyberattacks to a particular state or non-state actor, which has a multitude of implications. Tsagourias identifies three characteristics of cyberspace that make attribution difficult: the ability for attackers to hide their identities, the fact that attacks can be undertaken by multiple people in multiple jurisdictions simultaneously, and the speed at which cyberattacks can take place (2012: 233-34). There are also anti-attribution tools being developed which mask the origin of the attack, making it more difficult for the targets of cyberattacks to identify the responsible actor (Tsagourias,

2012: 233-34). Cyberspace and anti-attribution tools provide a layer of plausible deniability, which create an incentive for states to use non-state actors as proxies, thus further obscuring their role in cyberattacks (Klimburg, 2011: 41-42; Maurer, 2015: 79).

This incentive leads states to ignore the illicit activities of proxy organizations because they need their capabilities in order to undertake attacks on their enemies (Klimburg, 2011: 42). In China, the government works directly with "patriot hackers" to engage in internal repression, while Russia has strong connections with cybercriminals whose goal is to engage in cyber activities to earn a profit, which includes stealing information from organizations and states in the West (Klimburg, 2011: 44-51). However, it is not just authoritarian countries that work with non-state actors. The United States government also works closely with the defence-industrial industry to develop technologies for intelligence gathering, cyberdefence, and offensive actions (Klimburg, 2011: 51-53).

The reason for Russia's particular interest in cyberattacks is notable due to its recent history. The country felt a need to catch up to the military capabilities of foreign states, and saw the use of cyberspace to conduct "information operations" as a way to get ahead in a critical and emerging area (Erol & Oguz, 2015: 268-69; Giles, 2011: 50-51). However, finding military recruits who are also able to conduct cyberattacks is proving difficult, which is why Russia has embraced non-state actors and "loose network[s] of highly technically capable individuals working towards a common goal" (Giles, 2011: 55). Makarychev associates the emphasis placed on military strength with Russia's desire to be acknowledged as a global hegemon and have the former Soviet states recognized as within their sphere of influence (2014: 182-85).

However, cyberattacks are rarely used by just one actor in modern warfare or civil wars. Ukraine has also engaged in cyberattacks and cyberdefence, however its efficacy has been questionable due to the country's inexperience relative to Russia. The Ukrainian government has not been able to effectively utilize the non-state capabilities at its disposal, and while it was able to mobilize hacktivist groups, it largely failed to incentivize cybercriminal groups to change their behaviour. Further, like Russia, the Ukrainian government has also decided not to prosecute the illegal activities undertaken by cyberattackers because of how they can assist the government in conducting attacks against their enemies (Maurer, 2015: 84-85).

Within the literature on cyberattacks, the most central discussion revolved around the challenging nature of attributing these crimes to their rightful owner. The nature of cyberspace makes it difficult to identify the responsible actor or even where the attack originated, and anti-attribution tools only make this task more challenging. It is also important to examine the types of attacks and possible impacts they can have. For this reason, the Ukrainian case study will focus on cyberattacks on critical infrastructure, since they carry the largest possibility of destruction and can potentially be considered armed attacks which could justify retaliation under international law. Cyberattacks have been an important element of the war in Ukraine, but the actual specifics of the conflict are even more complex.

Case study: Ukraine

The conflict underway in Ukraine has been deemed a civil war by the Uppsala Conflict Data Program since it exceeded 1000 deaths per year in both 2014 and 2015. It began after a series of events in early 2014, which fiercely divided the country along pro-European and pro-Russian lines.

Ukrainian President Viktor Yanukovych was deposed in February 2014 after refusing to sign an association agreement with the European Union, and instead pivoted to seek closer ties with

Russia, which provoked Ukrainians primarily in the west of the country to engage in mass demonstrations. However, pro-Russian Ukrainians were angry about these developments and began to protest in Crimea and the eastern parts of the country. In late February 2014, Russian "little green men"—soldiers who were not wearing insignia or identification—seized government buildings in Crimea and a referendum for independence was held in mid-March, before Russia finally annexed the region on March 18, 2014 (Erol & Oguz, 2015: 269-71).

The civil war began in the months after the annexation of Crimea when two independence movements emerged out of the protests in the east: the Donetsk and Luhansk People's Republics. They demanded sovereignty from the pro-European Ukrainian government in order to develop deeper relationships with Russia. This was in line with the Russian desire to "reassembl[e] the fragmented world of Russian-speakers" (Makarychev, 2014: 186). The primary dyads within the civil war have been between the Ukrainian government and the respective Donetsk and Luhansk People's Republics. However, since the Ukrainian civil war has been internationalized as a result of Russian inference, there is also a dyad, which includes the governments of Ukraine and Russia, who are largely to blame for the cyberattacks undertaken by both sides. Since the laws around cyberattacks do not seem to be concrete, it is difficult to provide solid evidence that either of these states is actually responsible for a particular attack. The most prominent cyberattacks that have taken place have all had the impact of disrupting the actions of the Ukrainian government.

During the May 2014 Ukrainian presidential election, hacktivist group CyberBerkut compromised the Central Election Commission. As a result, the real-time voter counter did not work properly for 20 hours, and the group posted false information to the Commission's website claiming that the leader of the far-right nationalist Right Sector party had won the election—a claim that was immediately broadcast on Russian television (Koval, 2015: 56-57). Those who undertook the attack were experts, as they also compromised many other election-related websites, and advanced cyber espionage malware was later found on the Commission's servers (Koval, 2015: 57). In line with the literature, while there was heavy suspicion that Russia was involved with the attack through a proxy due to its sophistication and the swift broadcasting of the false information, it was impossible to gather the necessary evidence to prove the claim.

There was a similar lack of evidence to support Ukraine's claim that Russia had attacked its power grid in December 2015 (Zetter, 2015). 230,000 Ukrainians were left without power when hackers compromised three power control centres, eventually taking approximately sixty substations offline, as well as the backup power at two of the control centres. Passwords were changed to lock out the operators, and the attackers replaced legitimate firmware with malicious firmware, leaving substations unable to receive remote commands. They even launched a DoS attack against call centres so they could not receive calls from customers, and flooded their lines with bogus calls, which appeared to come from Moscow (Zetter, 2015). Despite no concrete evidence to support Russian involvement that did not stop the Ukrainian government from making the claim. Zetter explained that, an attack could have been seen as retaliation for a physical attack by pro-Ukrainian activists on substations feeding power to Crimea, but the attack had been in the planning stages for several months, which makes this explanation unlikely (2015). A second cyberattack on the Ukrainian power grid took place in December 2016, cutting off a fifth of the power to the capital city of Kiev, and while there were similarities between the two attacks, there was again inconclusive evidence to link it directly to the Russian government (BBC, 2017).

This second strike on the power grid was part of a larger campaign of cyberattacks that occurred in November and December 2016, during which time the Ukrainian government claimed state institutions had experienced more than 6,500 cyberattacks, including an attack on the State

Treasury that left employees and pensioners unable to receive their salaries and payments (Zinets, 2016). Ukraine's president again claimed that Russia was, "directly or indirectly … waging a cyberwar against our country," yet could provide little evidence because of the nature of cyberspace (Zinets, 2016). Further attacks on the financial system and the power grid were reported in early 2017, when Ukraine also claimed that even more sophisticated viruses were being used in the attacks (Zinets, 2017).

The cyberattacks undertaken against Ukraine, in the context of the ongoing civil war, reflect many of the aspects found in the literature. While the Ukrainian government wishes to identify Russia as the culprit, either directly or through proxies, it is unable to find the evidence to make such claims because of the difficulty of attribution associated with cyberattacks.

Minor attacks are not often reported, even though they make up the bulk of the cyberattacks that occur; yet the relatively small number of attacks on critical infrastructure has a potentially more significant impact. These attacks can potentially disable core government functions, while leading the population to have less trust in its government to reliably deliver services and provide security.

Conclusion

The impacts of cyberattacks on civil wars are still being understood by researchers, yet the application of existing literature to the ongoing Ukrainian civil war evidences that several primary factors are present. Cyberattacks are undertaken by proxy groups, making it more difficult for the state that has been attacked—in this case Ukraine—to determine, or prove, which group or state is ultimately responsible. Attacks on critical infrastructure can also have significantly larger effects than more simple DoS attacks, and can undermine the trust of the population in their government.

What does remain rather unknown, however, is what impact cyberattacks have on the length or severity of conflicts. In the Ukrainian civil war, cyberattacks are assumed to have largely been carried out by proxies under the direction of the Russian government in support of the pro-Russian separatists and against the Ukrainian government, not by the separatists themselves. Buhaug, Gates, and Lujala found that the proximity of rebels to international borders, whether they were located in a peripheral area of the country, and their weakness relative to government forces were predictive of longer conflicts (2009: 559-63). When applied to Ukraine, this would indicate a longer conflict, since the separatists are located near the Russian border and are in a peripheral eastern area of the country; yet while they are weaker than the Ukrainian government, they also have the support of Russia, which may equalize the playing field or give the separatists an advantage. The degree to which cyberattacks may provide an advantage for the separatists over the Ukrainian government remains unknown.

As more state and non-state actors develop the capabilities to engage in cyberattacks, thus impacting the dynamics and duration of civil wars, researchers will have to make use of the resources at their disposal to attempt to understand how negative impacts may be mitigated. As cyberattacks become even more common, it will be important to understand whether they have an impact on the duration of conflicts, and whether they affect their casualty rates. It is possible that the ability to take out critical infrastructure from significant distances could alter their lethality, but cyberattacks may also provide the weaker side of the dyad a way to somewhat equalize the power distribution if they have advanced technological skills. There are many questions surrounding the impact of cyberattacks on civil wars, and due to the speed at which these technologies are developing, researchers may always find themselves trying to keep up with new

developments, as they attempt to keep their research current in an effort to find ways to lessen the length and lethality of on-going conflicts. At least that would be the hope.

References

Buhaug, Halvard, Scott Gates and Päivi Lujala. 2009. "Geography, rebel capacity, and the duration of civil conflict." *Journal of Conflict Resolution* 53: 544-69.

Erol, Mehmet S. and Safak Oguz. 2015. "Hybrid warfare studies and Russia's example in Crimea." *Journal of Gazi Academic View* 9: 261-77.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu and Phillip Laplante. 2011. "Dimensions of cyber-attacks: Social, political, economic, and cultural." *IEEE Technology and Society Magazine* 30: 28-38.

Giles, Keir. 2011. "'Information troops' – a Russian cyber command?" Paper presented at the 3rd International Conference on Cyber Conflict, Tallinn.

Klimburg, Alexander. 2011. "Mobilising cyber power." *Survival* 53: 41-60.

Koval, Nikolay. 2015. "Revolution hacking." In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers. Tallinn: NATO CCDCOE Publications.

Makarychev, Andrey. 2014. "Russia, Ukraine and the Eastern Partnership: From common neighorhood to spheres of influence?" *Insight Turkey* 16: 181-99.

Maurer, Tim. 2015. "Cyber proxies and the crisis in Ukraine." In *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers. Tallinn: NATO CCDCOE Publications.

Tsagourias, Nicholas. 2012. "Cyber attacks, self-defence and the problem of attribution." *Journal of Conflict & Security Law* 17: 229-44.

"Ukraine power cut 'was cyber-attack'." 2017. *BBC*, January 11. *http://www.bbc.com/news/technology-38573074* (March 20, 2017).

"Ukraine." n.d. Uppsala Conflict Data Program. *http://ucdp.uu.se/#country/369* (March 22, 2017).

Zetter, Kim. 2016. "Inside the cunning, unprecedented hack of Ukraine's power grid." *Wired*, March 3. *https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/* (March 28, 2017).

Zinets, Natalia. 2016. "Ukraine hit by 6,500 hack attacks, sees Russian 'cyberwar'." *Reuters*, December 29. *http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN14I1QC* (March 22, 2017).

Zinets, Natalia. 2017. "Ukraine charges Russia with new cyber attacks on infrastructure." *Reuters*, February 15. *http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN* (March 22, 2017).