ISN
ETH Zurich

17 October 2014

The Russia-Ukraine Conflict: Cyber and Information Warfare in a Regional Context

What lessons can we learn from Russia's cyber and information campaigns against Ukraine? According to Tim Maurer and Scott Janz, we should expect them to become more integrated, especially in hybrid conflicts, and we need to face facts — Russia has only revealed the tip of the iceberg when it comes to its cyber capabilities.

By Tim Maurer and Scott Janz for ISN

The violent conflict between Russia and Ukraine that broke out earlier this year has become a case study for hybrid conflict, where traditional kinetic actions are shadowed by cyber and information warfare activity. Now that the Ukrainian and Russian governments have agreed to terms on a peace plan, it is a good moment to reflect on how this conflict unfolded and what it can teach us about the use of cyberspace during a conflict that lasted several months.

First, it is important to remember that the Russian annexation of Crimea is not the first instance in the region where traditional military engagement occurred in parallel with Internet based hostile activity. During the 2008 Russia-Georgia War, for example, botnets were used while kinetic military operations were taking place to deface websites and to conduct Distributed Denial of Service (DDoS) attacks, which overwhelmed websites and rendered them inaccessible. These actions primarily targeted Georgian government and news media websites, disrupting communication channels and generating confusion at a time of crisis. It is evident that many of these strategies have been redeployed in Ukraine, while others have reached new levels of sophistication.

The use of cyberspace in the Ukrainian conflict is particularly interesting because it combines both cyber and information warfare tactics. This includes tampering with fiber-optic cables and with the cell phones of Ukrainian parliamentarians, as well as more common malicious tools such as DDoS attacks and web defacements. The range of this activity illustrates how cyber warfare can be distinguished from information warfare, and suggests that future kinetic actions are likely to be accompanied by both.

Background: The use of cyberspace as the conflict was escalating

The simmering political tension inside Ukraine escalated in November 2013, when former Ukrainian president Viktor Yanukovych abandoned plans to sign a trade agreement with the EU. Many believed this was a sign that he was seeking closer ties with Moscow. Yanukovych's decision incited mass protests that were met with a violent government crackdown. This sudden outbreak of violence

deepened existing fault lines in the country split between those favoring Moscow in the east and those favoring the European Union in the west.

Long before Yanukovych's flight in February and the buildup of Russian troops on the Crimean border, pro-Russian separatists began a concerted effort to discredit pro-European Ukrainians. Beginning in late November, reports emerged that Russian hacker groups were defacing and executing DDoS attacks on websites critical of the Yanukovych government's relationship with Russia. This period was characterized by low-level hacking targeting highly visible websites, either rendering them unavailable or changing their content.

This activity took place as Yanukovych was trying to quell the growing civil unrest against his government. In addition to the use of police violence, the Yanukovych government also leveraged its control of the national telecommunications infrastructure to intimidate protestors. In late January, for example, people in the vicinity of clashes between riot police and protestors received an ominous text message on their cellphones containing the warning: "you are registered as a participant in a mass disturbance." While unsigned, the messages were widely believed to have been sent by the Yanukovych government. This activity was part of a mounting information campaign aimed at creating or changing the content people were consuming to influence their opinion. This campaign would intensify as the conflict escalated over the coming months. However, Yanukovych was eventually forced to flee the country and Moscow became more involved.

Cybered conflict: The use of cyberspace during the hot conflict

On February 28, shortly after Yanukovych had left the country, unmarked soldiers, whom Russia's President Putin later acknowledged to be Russian troops, seized a military airfield in Sevastopol and the Simferopol international airport. Concurrently, armed soldiers tampered with fiber optic cables, raiding the facilities of Ukrainian telecom firm Ukrtelecom, which stated afterward that it had "lost the technical capacity to provide connection between the peninsula and the rest of Ukraine and probably across the peninsula, too." In addition, cell phones of Ukrainian parliamentarians were hacked and the main Ukrainian government website was shut down for 72 hours after Russian troops entered Crimea on March 2. Patriotic Ukrainian hacker groups such as Cyber Hundred and Null Sector retaliated with DDoS attacks of their own against websites of the Kremlin and the Central Bank of Russia.

While the jamming of communication channels has been a standard practice of militaries since the advent of communication technologies, cyberspace has enabled new ways to influence a conflict's outcome. For example, a report released in March by BAE, a British defense and security firm, revealed that dozens of computers in the Ukrainian prime minister's office and several embassies outside of Ukraine had been infected with malicious software called Snake capable of extracting sensitive information. While the operators of the Snake malware were located in the same time zone as Moscow, and Russian text was found in its code, the evidence that the malware originated in Russia is circumstantial . Nevertheless, these intrusions illustrate how the use of cyberspace became increasingly aggressive, shifting from trying to manipulate content to physically tampering with cables and targeted hacks that supported the Russian invasion.

As the March 16 referendum on the fate of Crimea neared, Russian hackers ramped up their campaign to discredit Ukrainian officials. This broader misinformation campaign sought to mobilize political support and discredit opponents leading up to the referendum on the region's status in March. Similar tactics were used before the election in May to determine Yanukovych's successor. As described by James Lewis of the Center for Strategic and International Studies, "Russia's strategy is [to] control the narrative, discredit opponents, and coerce." In fact, the day before the presidential election, Ukraine's Security Service discovered a virus in the systems of the Central Election

Commission designed to compromise data collected on the results of the election, revealing how close Russian hackers had come to sabotaging the results. Cyber Berkut, the same group responsible for the DDoS attack against three NATO sites in March, claimed responsibility for the attack.

While Ukrainian government officials and many news reports blame the Russian government for indirectly orchestrating these operations, as well as for the crude 'hack attacks' on Ukrainian state websites, the Russian government has vehemently denied accusations that they have any influence over these groups. Details about the relationship between pro-Russian separatists or hacker groups such as Cyber Berkut and the Russian government remain lacking. However, paralleling the conflict in Georgia, the timing of the simultaneous cyber and kinetic attacks suggests a minimum level of coordination, raising doubts regarding the Russian government's statements.

Other important pieces of this puzzle remain murky, as well: some speculate that the Russian government may possess unfettered access to the Ukrainian telecommunication system, as the Ukrainian intercept system closely resembles that used by Russia. Moreover, several observers have argued that the Russian government has demonstrated a considerable amount of restraint in the region in its use of cyberspace during the conflict. This seems plausible given that the Russian military has demonstrated that it can move in and out of the peninsula relatively unimpeded. Indeed, the Russian government has had little incentive to reveal its full military capabilities, including its cyber arsenal.

Implications

It is worth briefly discussing the broader international ramifications of this. In particular, it is worth noting that at the NATO summit in early September, NATO member states officially declared that "Cyber attacks can reach a threshold that threatens national and Euro-Atlantic prosperity, security, and stability. Their impact could be as harmful to modern societies as a conventional attack. We affirm therefore that cyber defence is part of NATO's core task of collective defence. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis." This declaration is the culmination of the debate over Article 5 and cyber attacks which started after the Estonian experience in 2007. NATO also provided $20 million in 'non-lethal' aid to Ukraine in September with a focus on cyberdefense.

In short, the events in Ukraine as well as in Georgia in 2008 and in Estonia in 2007 have offered the world a glimpse at Russia's cyber capabilities. Moreover, the conflict in Ukraine has demonstrated that in the digital age, kinetic action is likely to be accompanied with information and cyberwarfare – in Eurasia and elsewhere.

For more information on issues and events that shape our world, please visit the ISN Blog or browse our resources .

Tim Maurer is a non-resident fellow at the Global Public Policy Institute (GPPi) and a research fellow at the New America Foundation's Open Technology Institute in Washington DC. Prior to joining the New America Foundation, Tim was a research associate at the Center for Strategic and International Studies, where he continues to be an adjunct fellow.

Scott Janz is an intern at New America's Open Technology Institute where he conducts research on

cybersecurity and Internet governance. He is currently completing his M.A. in Global Governance at the Balsillie School of International Affairs in Waterloo, Canada, focusing on risk and uncertainty management.

Publisher

International Relations and Security Network (ISN)

---

http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=184345&lng=en

---

ISN, Center for Security Studies (CSS), ETH Zurich, Switzerland